

Military Intelligence

Production Requirements and Threat Intelligence Support to the U.S. Army

**Headquarters
Department of the Army
Washington, DC
28 June 2000**

UNCLASSIFIED

SUMMARY of CHANGE

AR 381-11

Production Requirements and Threat Intelligence Support to the U.S. Army

This regulation--

- o Established threat support responsibility for Space Missile Defense Command (SMDC) (chap1).
- o Establishes co-authority for validation of Army Production Requirements (PRs) (chap 2).
- o Updates relevant terms (throughout reg).
- o Changes previous title of AR 381-11 (title page).
- o Requires Threat documentation for COTS products in Major Automated Information Systems (AIS/MAIS) (chap 1).
- o Requires mandatory System Threat Assessment Reports (STARS) for Special Access Programs (SAPS) (chap 3).

Effective 19 July 2000

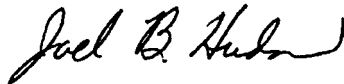
Military Intelligence

Production Requirements and Threat Intelligence Support to the U.S. Army

By Order of the Secretary of the Army:

ERIC K. SHINSEKI
General, United States Army
Chief of Staff

Official:



JOEL B. HUDSON
Administrative Assistant to the
Secretary of the Army

History. This printing publishes a revision of AR 381-11 and replaces AR 381-19.

Summary. This regulation contains the procedures for requesting intelligence and threat intelligence support for various applications in the Army to include: analyses, automated information systems, life-cycle management, technology, studies, simulations, simulators, computer models,

battle labs, force, combat, materiel developers, and training development.

Applicability. This regulation applies to major Army commands, National Ground Intelligence Center, Department of the Army Staff, Program Executive Offices, Army Operating Agencies, Reserve Component units and individuals augmenting major Army commands, when requesting new intelligence production. This regulation also applies to all Army customers when requesting production of intelligence concerning foreign threats. All intelligence requirements and production must comply with AR 381-10, U.S. Army Intelligence Activities and Executive Order 12333.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff for Intelligence (DCSINT). The DCSINT has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation. The DCSINT may

delegate this approval authority, in writing, to a deputy director within the proponent agency in the rank of colonel or the civilian equivalent.

Army management control process. This regulation contains management control provisions and identifies key management controls that must be evaluated in accordance with AR 11-2.

Supplementation. Supplementation of this regulation and establishment of command or local versions are prohibited without prior approval from HQDA (DAMI-FIT), 2511 Jefferson-Davis Highway, Presidential Towers, Suite 9300, Arlington, VA 22202-3910.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQDA, (DAMI-FIT) 2511 Jefferson-Davis Highway, Presidential Towers, Suite 9300, Arlington, VA 22202-3910.

Distribution. This publication is available in electronic media only and is intended for command level D.

Contents (Listed by paragraph and page number)

Chapter 1

Introduction, page 1

Purpose • 1-1, page 1

References • 1-2, page 1

Explanation of abbreviations and terms • 1-3, page 1

Responsibilities • 1-4, page 1

Policies • 1-5, page 6

Chapter 2

How To Obtain Intelligence, page 9

Section 1

Obtaining Existing Intelligence Products and the Intelligence Dissemination Program, page 9

General • 2-1, page 9

Intelligence Dissemination Program • 2-2, page 9

INSCOM • 2-3, page 9

Approval recommendations • 2-4, page 10

*This regulation supersedes AR 381-11, dated April 1993 and AR 381-19, dated February 1988.

Contents—Continued

Establishing a DIA intelligence dissemination customer account • 2–5, *page 10*
Updating the SII, SIGINT end products (SEP) and current intelligence (CURINTEL) accounts • 2–6, *page 10*
Obtaining secondary dissemination • 2–7, *page 10*
Obtaining human intelligence reporting • 2–8, *page 10*
Obtaining recurring electrically disseminated intelligence products • 2–9, *page 11*
Obtaining SIGINT end product (SEP) • 2–10, *page 11*
Requesting approved intelligence product distribution lists • 2–11, *page 11*

Section II

Obtaining New Intelligence Production, page 11
The production requirement process peacetime • 2–12, *page 11*
Guidance to customers when preparing production requirements • 2–13, *page 14*
Guidance when preparing a production center response • 2–14, *page 18*

Chapter 3

Threat Intelligence Support, page 20

Section I

Threat Intelligence Support Programs, page 20
General • 3–1, *page 20*
Intelligence products • 3–2, *page 21*
Threat intelligence in modeling and simulation • 3–3, *page 21*
Threat simulators and targets • 3–4, *page 22*
Threat scenario development • 3–5, *page 22*
Threat Integration Staff Officer (TISO) • 3–6, *page 22*
System Threat Analyst responsibilities (DAMI-FIT) • 3–7, *page 23*
Threat coordinating groups (TCGs) • 3–8, *page 24*
Threat assessments • 3–9, *page 24*
System threat assessment report (STAR) • 3–10, *page 25*
STAR ACAT II-IV • 3–11, *page 26*
Threat test support package (TTSP) • 3–12, *page 27*
Analysis of Alternatives (AOA) • 3–13, *page 28*
Special Access Programs (SAPs) • 3–14, *page 28*

Section II

Army Studies, page 28
Army studies • 3–15, *page 28*
Other Army plans and strategy documents • 3–16, *page 29*
Technology • 3–17, *page 29*
Army Battle Lab • 3–18, *page 30*

Appendixes

- A.** References, *page 36*
- B.** System Threat Assessment Report Format, *page 37*
- C.** Threat Test Support Package (TTSP) Format Guidance, *page 42*

Table List

Table 1–1: Threat Support Responsibilities Matrix, *page 7*

Figure List

Figure 2–1: The Requirements Process Peacetime, *page 13*
Figure 2–2: The Requirement Process Crisis/War, *page 14*
Figure 2–3: Production Requirements, *page 16*

Contents—Continued

- Figure 2–3: Production Requirements—Continued, *page 17*
- Figure 2–3: Production Requirements—Continued, *page 18*
- Figure 2–4: Production Center Response, *page 20*
- Figure 3–1: Threat support to force, combat, and material development, *page 30*
- Figure 3–2: Threat support to developmental and operational testing, *page 31*
- Figure 3–3: STAR production & validation process (ACAT I programs through MS I), *page 32*
- Figure 3–4: STAR production & validation process (ACAT I programs through MS II), *page 33*
- Figure 3–5: Threat test support package (TTSP) validation process, *page 34*
- Figure 3–6: Analysis of Alternatives (AOA) validation process, *page 35*
- Figure B–1: Critical Intelligence Category (CIC) examples, *page 41*
- Figure B–2: STAR Cover page (format), *page 42*

Glossary

RESERVED

Chapter 1

Introduction

1-1. Purpose

This regulation prescribes Army policy and procedures and assigns responsibilities for:

a. Obtaining intelligence products. Establishes processes by which Army policy-makers, warfighters, major Army commands (MACOMs), the Army staff, Army operating agencies, force modernization and planning activities and a host of other organizations obtain available published intelligence; prepare production requirements (PRs) to obtain answers to intelligence questions; and explains how customers receive responses to PRs in the form of intelligence products they need to perform their mission.

b. Multi-Disciplined Intelligence support. Providing Multi-Disciplined Intelligence support (MDI) to Army force, combat, materiel, and training development and provide policies, responsibilities, and procedures for threat intelligence support to modeling and simulation, simulator and target development, non-developmental items (NDI), Commercial-Off-The-Shelf (COTS), and technology based programs to include Advanced Technology Demonstrations (ATDs), Advanced Concept Technology Demonstrations (ACTDs), and Horizontal Technology Integration (HTI) efforts. This regulation is intended to ensure that MDI support guides the Army's force modernization efforts through the 21st century.

c. Department of Defense 5000.2-R. Requires the threat to automated information systems be identified and quantified early in the acquisition life cycle. This regulation implements this requirement by applying the intelligence process to identify the threat to automated information systems developed under Department of Defense Directives (DOD) 5000.1 and 5000.2 (Defense Acquisition).

1-2. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

1-3. Explanation of abbreviations and terms

Abbreviations and special terms used in this regulation are explained in the glossary.

1-4. Responsibilities

a. The Deputy Chief of Staff for Intelligence (DCSINT) has Army Staff responsibility for determining intelligence priorities and for managing the production of intelligence by the National Ground Intelligence Center (NGIC) and establishing MDI support policy and guidance for the Army. The DCSINT exercises this responsibility through the Foreign Intelligence (DAMI-FI) Directorate and U.S. Army Intelligence and Security Command (USAINSCOM). The DCSINT serves on the Army Systems Acquisition Review Council (ASARC).

(1) The Director, Foreign Intelligence (DAMI-FI) will—

(a) Develop and interpret Army Intelligence Production policy in line with DOD, the Intelligence Community and Army goals for the Army production program.

(b) Serve as the Army Functional Manager for Intelligence Production which includes analyzing, developing, justifying and representing the Army Intelligence Production Program as a portion of the General Defense Intelligence Program.

(c) Manage the Quality of Analysis Program for HQDA, ODCSINT to ensure that analytic professional development needs are met.

(d) Serve as the program manager and executive secretary of the Production Resource Allocation Board for HQDA, ODCSINT to ensure proper utilization of reserve component production augmentation resources to support both peacetime and contingency intelligence production.

(e) Monitor and exercise oversight of the Army production validation and dissemination functions performed by HQ, Intelligence and Security Command (INSCOM) on behalf of the DCSINT, HQDA.

(f) Represent the DCSINT, HQDA at national and DOD intelligence production such as the National Intelligence Production Board and the Defense Intelligence Production Council.

(g) Conduct Army production reviews to monitor production center responsiveness to PRs generated by Army customers and to assess the intelligence community response in support of Army's Priority Intelligence Needs.

(h) Serve as the ODCSINT representative to the Army Priority Intelligence Needs Coordinating Group.

(2) The Foreign Intelligence Director of Threat (DAMI-FIT) will—

(a) Approve and/or coordinate threat documentation designated for ASARC or Defense Acquisition Board (DAB) decisions, studies, and testing in support of the Department of the Army (DA) decision process. (See Table 1-1 for threat support responsibilities matrix.)

(b) Review and monitor the MDI support process to ensure consistent application of MDI in support of Acquisition Category (ACAT) I and II programs (DOD 5000.2-R), and Class I-III information systems, selected Director, Office of the Secretary of Defense Test and Evaluation (OSD T&E) oversight systems, DA-directed studies, technology efforts, and selected combat developer-directed studies.

(c) Establish and chair HQDA Threat Coordinating Groups (TCGs) for ACAT I and II systems (DOD 5000.2-R), automated information systems, ACTDs, ATDs, and other efforts such as red teams and Advance Warfighting Experiments (AWEs).

(d) For Joint Programs (JPs) in which the Army is the lead Service, coordinate System Threat Assessment Reports (STARs) with other Service participants prior to submission to Defense Intelligence Agency (DIA) for validation. For JPs in which the Army is a participant, but not the lead Service, coordinate and assist the designated lead Service in accordance with that Services' regulations. Appropriate coordination is also required for combined (multi-country) programs.

(e) Provide Threat Integration Staff Officer (TISO) and/or analyst representation in appropriate TCGs, other service Threat Steering Groups (TSGs), Test Integration Working Groups (TIWGs), Validation Working Groups (VWGs), and Threat Accreditation Working Groups (TAWGs) under TIWG auspices for ACAT I and II programs, for information systems, for selected OSD T&E oversight systems, DA-directed studies, technology efforts, and selected combat developer-directed studies. Representation also includes Integrated Concept Teams (ICTs), Integrated Product Teams (IPTs) as appropriate. TISOs will actively support testing of ACAT I and II systems in the early planning for threat support.

(f) Represent the Army at Intelligence Community briefings to remain current with the threat to the Army. Further, review the threat in the Mission Need Statement (MNS), Operational Requirements Document (ORD), Modified Integrated Program Summary (MIPS), Test and Evaluation Master Plan (TEMP), Analysis of Alternatives (AOA) and System Threat Assessment Report (STAR).

(g) Review intelligence data for ACAT IC (milestone decision reviews (MDRs) II-IV) programs and for ACAT II (MDRs I-IV) programs. (See Table 1-1.)

(h) Serve as the Army studies program focal point for ODCSINT and provide for representation to special task forces (STFs), special study groups (SSGs), study advisory groups (SAGs), General Officer Steering Committees (GOSC), and other study efforts requiring S&TI support.

(i) Establish and chair HQDA TCGs for program objective memorandum (POM) related study programs. (For example, ammunition stocks required to counter a threat.)

(j) Ensure that necessary threat databases are developed and maintained to facilitate management of the S&TI support process.

(k) Approve threat documentation for systems designated for examination by the Major Army Information System Review Council (MAISRC).

(l) Review and monitor the threat support process to ensure consistent application of threat in support of all automated information systems.

(m) Serve as a member of the MAISRC.

(n) Monitor responsiveness to PR generated as a result of the development of STARs to support the acquisition life-cycle of major automated information systems.

(o) Provide TISO representation in appropriate TIWG for all automated information systems.

(p) Review and validate threat intelligence in support of technology based efforts.

(3) Director, Foreign Intelligence Area (DAMI-FIA) will—

(a) Represent Army on production related issues within the National Intelligence Community, including management of all Army involvement in National Intelligence Council products and representing the DCSINT on the National Foreign Intelligence Board.

(b) Serve as the Army Staff proponent for general military intelligence (GMI) studies, analyses, and forecasts on global/regional threat trends, developments, and issues. Represents ODCSINT on related STFs, SSGs, SAGs, GOSCs, and other efforts requiring GMI support.

(c) Ensure necessary GMI threat databases are developed and maintained to facilitate management of the GMI support process.

(d) Convene study groups, working groups, TCGs, as required to develop and review GMI analyses and to ensure that intelligence data on threat doctrine, projections, developments, issues, and force employment are logical and consistent.

(4) The U.S. Army Intelligence and Security Commander (INSCOM) will—

(a) On behalf of DCSINT, HQDA manage Army PRs and dissemination responsibilities under the Department of Defense Intelligence Production Program (DODIPP).

(b) Act as the DOD Dissemination Program Manager (DPM) for all Army customer accounts.

(c) Validate and assign Army PR for the Department of the Army per the DODIPP.

(d) Develop, coordinate, and implement procedures to execute these functions.

(e) Provide training as required to Army elements on all aspects of obtaining intelligence.

(f) Ensure that timely counterintelligence support is provided to DAMI-CH, DAMI-FI, materiel and combat developers, and organizations engaged in technology based efforts.

(g) Acquire foreign materiel for S&TI exploitation program and for use in exploitation which is beneficial in

research, development, and testing, for developing simulators and surrogates for use as targets in support of developmental and operational tests, training, and for protecting our forces.

b. The Deputy Chief of Staff for Operations and Plans (ODCSOPS) has the General Staff responsibility for determining Army priorities for intelligence. This responsibility is executed through the activities of the Army Priorities Intelligence Needs Coordinating Group (APINCG). The Army intelligence priorities are determined annually and are based on The Army Plan (TAP). A copy of the approved Army intelligence priorities is available by contacting DAMO-SSP or DAMI-POB. The DCSOPS serves on the JROC and ASARC. The DCSOPS will—

- (1) Coordinate with ODCSINT on requirements for MDI support to STFs, SSGs, study directives, analyses, and guidance documents.

- (2) Participate in DA-level TCGs for coordination of MDI as appropriate.

- (3) Coordinate with ODCSINT on appropriate MDI guidance and policy.

- (4) Coordinate with ODCSINT for training support requirements, including threat guidance and foreign materiel for training (FMT).

c. The Army Staff will submit requirements for MDI support to the DCSINT in accordance with this regulation.

d. The Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA(ALT)) will coordinate with ODCSINT—

- (1) For research, development, and acquisition requirements for MDI support to include STFs, SSGs, study directives, analyses, technology efforts and guidance documents that ASA(ALT) is responsible from earliest concept stages.

- (2) To ensure that the Integrated Program Summary (IPS) prepared to support milestone decision reviews for ACAT I and II systems contain or reference HQDA-approved threat assessments.

- (3) To ensure that intelligence assets are programmed to support long-range planning initiatives, and that plans reflect consideration of the threat.

- (4) To ensure that approved threat statements and appropriate threat guidance and policies are present in the materiel change management program.

- (5) Participate in DA-level TCGs for coordination of MDI support to the force, combat, and materiel development process supporting the life-cycle acquisition of automated information systems (DOD 5000.2-R), and in other TCGs as appropriate.

- (6) Ensure that appropriate intelligence data and approved threat assessments are integrated into developmental testing (DT) and operational testing (OT).

e. The MACOM commanders will—

- (1) Ensure each subordinate element registers a complete, current Statement of Intelligence Interest with the Army DPM and the National Military Intelligence System Center (NMISC).

- (2) Prepare, review, and transmit PRs per DODIPP and this regulation.

- (3) Review, annually all submitted PRs and registered SII, then cancel or supersede each PR, and update or cancel each SII.

- (4) Provide periodic assessments of how well intelligence production has addressed Army Priority Intelligence Needs (APINS) relevant to the commands mission.

- (5) Ensure that the appropriate threat documentation is prepared and approved for non-standard systems, developmental systems, NDI, and COTS or obtain HQDA, ODCSINT waiver.

f. The Program Executive Officers (PEO), Program Managers (PM), and developing agencies will—

- (1) Use appropriate MDI data throughout the acquisition life-cycle of a program.

- (2) Obtain MDI support through the appropriate supporting threat or intelligence office.

- (3) Identify to the supporting TRADOC, Threat Manager (TM), AMC Foreign Intelligence Officer (FIO), and to DCSINT for automated information systems, all intelligence support requirements, including those for threat statements for system program and decision documentation.

- (4) Incorporate validated and approved threat statements (fig 1-1) in each IPS, request for proposal (RFP), and Test and Evaluation Master Plan (TEMP) for all systems.

- (5) Develop, in coordination with the supporting TRADOC, TM, AMC, FIO, or DCSINT Critical Intelligence Categories (CICs) for each program.

- (6) Participate in TCGs and TAWGs, as appropriate.

- (7) Address threat risk management in presentations to the ASARC and DAB.

- (8) Chair Test and Evaluation Integrated Process Teams (TEIPTs) (PM responsibility).

- (9) Review STARS for system description in milestones II to IV.

- (10) Ensure that the appropriate threat documentation is prepared and approved for non-standard systems, developmental systems, NDI, and COTS technology or obtain HQDA, ODCSINT waiver.

- (11) Notify DAMI-FIT of the technical capabilities, limitations, and quantities of systems developed under Army auspices that become either co-development programs with a foreign government, or are identified for foreign military sales.

g. The Director, Test and Evaluation Management Agency (TEMA), will—

(1) Coordinate with ODCSINT on requirements for MDI support to threat targets (excluding range targets), simulators, and threat simulations that fall under the auspices of the CROSSBOW Program, STFs, and other guidance documents.

(2) Establish Army validation and accreditation policy for threat simulators, threat simulations, and threat targets.

(3) Charter validation working groups for threat simulators and threat targets.

(4) Ensure that threat representative targets and threat simulators are validated and accredited.

h. The Commanding General, Training and Doctrine Command (TRADOC) will—

(1) Prepare, review, coordinate with AMC, and forward to ODCSINT for HQDA approval all threat statements developed for each mission needs statement (MNS) and operational requirements document (ORD) for ACAT I and II, and OSD T&E oversight systems.

(2) Prepare, review, coordinate with AMC, and approve all threat statements developed for each MNS and ORD for ACAT III and IV systems. Provide information copies to ODCSINT, ATTN: DAMI-FIT.

(3) Prepare, coordinate with AMC, and forward all ACAT I STARs and ACAT II STARs to ODCSINT for review and approval within 180 days after MDR 0.

(4) Update STARs every 24 months or when significant changes in either the threat or U.S. system specifications and characteristics occur through MDR I. Obtain approval and validation for changes, revisions, or updates in accordance with Table 1-1.

(5) Coordinate on all AMC-prepared STARs subsequent to MDR I.

(6) Provide for MDI representation at each SSG and identify MDI support requirements to ODCSINT.

(7) Participate in appropriate TCGs, TEIPTs, TAWGs, and Red Team efforts.

(8) Establish and chair appropriate TCGs in coordination with AMC, to provide threat support to ACAT III and IV systems through MDR I.

(9) Prepare, in coordination with AMC, the STAR for ACAT III and IV systems through MDR I, unless specifically waived by TRADOC DCSINT. TRADOC DCSINT has approval authority for TRADOC proponent ACAT III-IV STARs through MDR I.

(10) Provide threat integration representation to TEIPTs and TAWGs for ACAT III and IV systems in coordination with AMC.

(11) Prepare Threat Test Support Packages (TTSPs) for Initial Operational Testing and Evaluation (IOT&E) and Operational Testing events requiring threat within DT when the DT and OT are combined. Coordinate TTSP development with AMC and ATEC. Ensure that threat portrayals are sufficiently realistic to satisfy test requirements. Approve TRADOC-developed TTSPs for IOT&E testing. Conduct on-site approval and validation of threat portrayals in operational test, and operational assessments occurring in developmental test. Coordinate TTSP development with AMC and ATEC. Coordinate threat approval and validation with ODCSINT on ACAT I and II programs. Forward TTSPs for approval in accordance with Table 1-1.

(12) Provide or review and approve threat and foreign intelligence used in TRADOC sponsored, or conducted studies (for example, AOAs, models, scenarios, databases, simulations and systems). Ensure that threat used is derived and documented from DIA or HQDA approved sources and is properly applied within designated specific contexts. Coordinate approval of threat/foreign intelligence products with DA DCSINT and DIA as appropriate. (See Table 1-1.)

(13) Provide threat support to TRADOC Integrated Concept Teams (ICTs).

(14) Prepare, review, and approve threat and/or Opposing Forces (OPFOR) products and depictions for training, Army-wide.

(15) Identify and submit command threat support requirements.

i. The CG, Army Material Command (AMC), will—

(1) Serve (through the supporting SIO/FIO) as the PEO/PM's sole source of MDI support through the entire life cycle of assigned programs developed in accordance with DOD 5000.1, 5000.2-R and 5000.39 and DIAR 55-3.

(2) Prior to MDR I, coordinate on all TRADOC-prepared STARs .

(3) Assume responsibility for ACAT I and II STARs production from TRADOC, coordinate AMC-produced STARs with TRADOC, and forward the coordinated ACAT I STARs and ACAT II STARs to ODCSINT for review and approval subsequent to MDR I.

(4) Serve as Army point of contact responsible for coordination of input to the Military Critical Technology List (MCTL).

(5) Update STARs at least every 24 months or when significant changes in either the threat or U.S. system specifications and characteristics occur subsequent to MDR I through MDR IV. Obtain approval and validation for changes, revisions, or updates in accordance with Table 1-1. Review and update as required every two years after MDR IV fielding of system.

(6) Prepare, in coordination with appropriate PEO/PMs, threat statements for IPS, RFP, TEMP, and in process reviews for ACAT I and II systems. Obtain ODCSINT approval for these threat statements.

- (7) Prepare, in coordination with TRADOC, the STARs for ACAT III and IV systems subsequent to MDR I, unless specifically waived by the AMC, ODCSINT.
 - (8) Prepare, in coordination with PEO/PM or developer, threat statements for IPS, RFP, and TEMPs for all ACAT III and IV systems. Provide information copies to ODCSINT.
 - (9) Identify and submit command threat support requirements.
 - (10) Document and submit CICs and related PRs identified by PEO/PMs and other developers.
 - (11) Participate in TEIPTs and TCGs. Ensure integration of approved MDI in developmental testing. Prepare TTSPs for developmental tests and ensure realistic MDI portrayals. Coordinate TTSP development with TRADOC.
 - (12) Participate in VWGs, TAWGs, and DA-level TCGs, as required. The AMC will chair TAWGs in support of DT.
 - (13) Establish appropriate TCGs for ACAT III and IV systems subsequent to MDR I, in coordination with TRADOC, as required.
 - (14) Determine threat documentation requirements for development programs under AMC purview and provide requisite support.
 - (15) Provide MDI support and guidance to technology base programs, to include Advanced Technology Demonstration (ATD), and Advanced Concept Technology Demonstration (ACTD) programs.
 - (16) Be responsible for engineering, development, acquisition, fielding, and capability accounting for Army targets, threat simulators, and major range instrumentation, other than those provided for by U.S. Army Space and Missile Defense Command (USASMDC). Develop simulators, simulation or surrogates instead of foreign materiel as required. Participate in VWGs and TAWGs.
 - (17) Prepare intelligence reports in accordance with Table 1-1.
 - (18) Review, approve, and ensure validation of threat inputs in AMC models, through the supporting FIO at the MSC or SRA running the models.
 - (19) Develop surrogates as necessary, instead of vulnerability, effectiveness and/or performance estimates for specific threat systems and munitions, where the required information for the specific threat is not yet available.
 - (20) Through the supporting FIO, submit via AMC, DCSINT to HQDA, DCSINT for approval a listing of proposed targets and munitions to be used in live fire tests.
- j. The Commanding General (CG), Space and Missile Defense Command (SMDC) will—
- (1) Lead efforts to prepare, review, coordinate with TRADOC elements and forward to HQDA, ODCSINT for approval all threat statements developed for support of Army space and National Missile Defense (NMD) requirements and experimentation efforts for designated ACAT I-IV systems.
 - (2) Coordinate, prepare, and review with TRADOC elements, and forward to ODCSINT for HQDA approval all threat statements developed for issues related to integration of Theater Missile Defense (TMD) efforts for designated ACAT I-IV systems.
 - (3) Identify and submit SMDC threat support requirements.
 - (4) Determine threat documentation requirements for development programs under SMDC purview and provide requisite support.
 - (5) Participate in appropriate TCGs, TEIPTs, and Red Team efforts.
 - (6) Provide threat support to the Space and Missile Defense Battle Lab (SMDBL).
 - (7) Review, approve, and ensure validation of threat inputs to SMDC models.
 - (8) Be responsible for engineering, development, acquisition, fielding, and capability accounting for Army targets, threat simulators, and major range instrumentation, as defined in Memorandum of Understanding (MOU) with AMC.
 - (9) Develop simulators, simulation or surrogates instead of foreign material as required. Participate in VWGs and TAWGs.
 - (10) Submit to HQDA, ODCSINT for approval a listing of proposed targets and munitions to be used in live fire tests.
 - (12) Prepare, review, coordinate with TRADOC threat reports in accordance with Table 1-1 for designated ACAT I-IV systems.
- k. The Commander, National Ground Intelligence Center (NGIC) and the Commander, Army Counterintelligence Center (ACIC) (when requested) will—
- (1) Produce and disseminate general military and scientific and technical intelligence as an integrated MDI product from multiple intelligence collection disciplines and function as either a primary, or a collaborative production center per the DODIPP.
 - (2) Produce intelligence to satisfy Army Title X responsibilities.
 - (3) Participate in the DOD shared production program.
 - (4) Participate in TCGs to support the force, combat, materiel, Army information systems, and training development process.

(5) As a primary production center, prepare a production center response (PCR) to every PR assigned by a validation office.

(6) When requested by the proponent, TM, FIO, or HQDA, DCSINT assist in the development of MDI and its application in selected combat and materiel developers' acquisition programs, studies, developmental and operational tests, combat training center (CTC) OPFOR portrayal, and models and simulations. When requested by the proponent, TM, FIO, or HQDA, DCSINT assist and focus on model sensitivity, decision logic performance, data input, scenario use, tactics, and doctrine.

(7) Provide threat data as required in support of VWGs and TAWGs.

(8) Provide representatives to DA and MACOM-level working groups, threat accreditation working groups and validation working groups for threat simulations and threat targets.

(9) Develop and maintain threat databases for PRs and CICs as directed by ODCSINT and INSCOM.

(10) Develop threat analysis and forecasting methodologies.

(11) Function as the authority for all threat data surrogate system data usage in support of Army analytic modeling efforts in coordination with ODCSINT.

(12) Provide foreign weapons system data to AMSAA for the production of weapon system performance information for use in Army analytical efforts. Review and approve the foreign weapon system performance information produced by AMSAA.

l. The CG, U.S. Army Test and Evaluation Command (ATEC) will—

(1) Coordinate test planning with the appropriate threat approval authority (Table 1-1) to ensure that a validated threat will be used in planning all ATEC managed activities.

(2) Participate in TCGs to ensure that MDI requirements to support testing are identified as early as possible after program initiation.

(3) Review and monitor all ATEC-managed testing activities and coordinate with TRADOC to ensure that the threat and OPFOR represented in testing conforms, to the extent feasible, with the validated threat.

(4) Maintain and operate threat simulators and targets in support of Army testing and training programs in a manner commensurate with threat force doctrine, tactics and operating procedures.

(5) Participate in VWGs, TAWGs, and DA-level TCGs, as appropriate. Chair TAWGs in support of operational testing.

(6) Employ validated targets, threat simulators, and target arrays in Army testing in accordance with the TTSP.

m. The Director, U.S. Army Concepts Analysis Agency (CAA) will coordinate with ODCSINT to ensure provision of appropriate MDI support to DA-sponsored force development studies.

n. The Director of Information Systems for Command, Control, Communications, and Computers (DISC4) will participate in DA-level TCGs focusing on threats to automated information systems developed or acquired under the purview of DOD 5000.1, 5000.2-R, 5000.39 and DIAR 55-3.

o. The U.S. Army Signal Commander (USASC) will—

(1) Prepare, review, and forward to ODCSINT for HQDA approval all threat statements developed for each MNS and ORD for all information systems, combat developed or material developed by the command, or upon request of a PEO or PM under matrix support arrangements.

(2) Prepare, review, and forward to ODCSINT for HQDA approval all STARs for information systems within 180 days after milestone decision review (MDR) 0 Defense Acquisition Board (DAB) approval.

(3) Update STARs for information systems prepared in accordance with paragraph 1-4o(1) above, every 24 months or when significant changes in either the threat or system specifications and characteristics occur subsequent to MDR I through MDR IV.

p. Other developers, testers and modelers not specifically identified in this regulation will ensure that OPSEC, multi-discipline counterintelligence (MDCI), foreign intelligence, and threat matters for their programs are addressed in accordance with specific program development regulations. Specific organizations identified in AR 70-1 with development responsibility include: U.S. Army Health Services Command, U.S. Army Signal Command (also, AR 25-1), U.S. Army Corps of Engineers, U.S. Army Criminal Investigation Command, and U.S. Army Strategic Defense Command.

1-5. Policies

a. Incorporating intelligence.

(1) Army customers will incorporate intelligence in support of mission requirements and the force, combat and materiel development threat assessment process in accordance with security restrictions specified in AR 380-5, AR 381-1, AR 380-381, AR 381-10 and AR 70-1.

(2) Commanders will obtain intelligence from organic and supporting organizations to the maximum extent possible before requesting dissemination or production of intelligence products in accordance with this regulation.

(3) Requests for dissemination and submission of production requirements will be expedited through command channels to the Army validation office, INSCOM (IAOP-OR-ITP).

b. Threat support to training, combat, force and materiel development.

(1) DOD Instruction (DODI) 5000.2-R contains guidance on threat support to materiel acquisition; it states that the objective is to ensure that each system developed is mission capable in its intended operational environment during its expected life.

(2) Defense Intelligence Agency Regulation 55-3 contains guidance on threat support to ACAT I programs for systems acquisition, and refers to procedures for ACAT II through IV programs.

(3) Policies for threat support to training, force, combat, and materiel development commands and system development organizations as they pertain to the Army are listed below.

(a) Consideration of threat intelligence is a command responsibility. Commanders, PEOs/PMs, other materiel developers to include the modeling and simulation community, combat developers to include TRADOC System Managers (TSMs), and study directors at all levels will ensure-via utilization of appropriate MDI authority-that MDI is applied and integrated into force, combat, materiel, simulation and modeling and training development programs.

(b) Multi-disciplined Intelligence, which includes scientific and technical intelligence characteristics, capabilities, and limitations of foreign equipment, and general intelligence (organization, doctrine, force structure, and tactics of threat forces), will primarily be derived from data sources with production responsibility as outlined in DOD-0000-151A-95 the Department of Defense Intelligence Production Program: Production Responsibilities. If other sources are used, such as, from unclassified open source publications or electronic on-line resources their use will be documented with justification and the source noted in the program or system-specific threat bibliography then approved through the intelligence channels listed in Table 1-1. The analysis of MDI data to meet threat requirements is the responsibility of the proponent threat support office and will be coordinated with HQDA, ODCSINT.

(c) Combat and materiel development commands and system development organizations (AR 70-1) will prepare required threat documentation, to include threat assessments, to support specific combat, materiel, automated information system, and training development activities for which those commands are responsible.

(4) Members of the Intelligence Production Community will provide intelligence support, in response to production requirements as dictated under DODIPP.

(5) The threat support activity (such as, the Threat Manager's Office (TM) for TRADOC; the Foreign Intelligence Directorate for Army Materiel Command (AMC); and the U.S. Army Space and Missile Defense Command (USASMD) Intelligence Division, DCSINT for USASOC and DCSINT of each command and activity involved in the force, combat, and materiel development process will review and approve threat assessments written in support of command missions before forwarding them to the next higher level of command.

Table 1-1
Threat Support Responsibilities Matrix

Document	Type of review	Milestone					Threat prepared by	Threat approved/validated by
		O	I	II	III	IV		
ACQUISITION CATEGORY 1D AND 1AM REQUIREMENTS								
MNS	ASARC/DAB	X					CBT DEV—Threat Manager	DA DCSINT/DIA
ORD	ASARC/DAB		X	X	X	X	CBT DEV—Threat Manager	DA DCSINT/DIA
MIPS	ASARC/DAB		X	X	X	X	MAT DEV	DA DCSINT/DIA
AOA ¹	ASARC/DAB		X	X	X	X	CBT DEV—Threat Manager	DA DCSINT/DIA
STAR	ASARC/DAB		X	X	X	X	CBT DEV—Threat Manager ²	DA DCSINT/DIA
TEMP	ASARC/DAB		X	X	X	X	MAT DEV—Foreign Intel Off ³ MAT DEV—Foreign Intel Off	DA DCSINT/DIA
TTSP	ASARC/DABX			X	X	X	CBT DEV ⁴	DA DCSINT/DIA
Intelligence Report	DAB	X	X	X	X	X	MAT DEV ⁴ DIA	Director, DIA
Validated Threat Statement	ASARC	X	X	X	X	X	DA DCSINT	DCSINT
ACQUISITION CATEGORY IC AND IAC REQUIREMENTS								
MNS	ASARC/DAB	X					CBT DEV—Threat Manager	DA DCSINT/DIA
ORD	ASARC/DAB		X	X	X	X	CBT DEV—Threat Manager	DA DCSINT/DIA 2
								DA DCSINT ³

Table 1–1
Threat Support Responsibilities Matrix—Continued

Document	Type of review	Milestone					Threat prepared by	Threat approved/validated by
		O	I	II	III	IV		
MIPS	ASARC/DAB	X	X	X	X		MAT DEV	DA DCSINT/DIA 2
								DA DCSINT ³
AOA ¹	ASARC/DAB ²	X	X	X	X		CBT DEV	DA DCSINT/DIA ²
STAR	ASARC ³							DA DCSINT ³
	ASARC/DAB ²	X	X	X	X		CBT DEV—Threat Manager ²	DA DCSINT/DIA ²
	ASARC ³						MAT DEV—Foreign Intel Off ³	DA DCSINT ³
TEMP	ASARC/DAB ²	X	X	X	X		MAT DEV—Foreign Intel Off	DA DCSINT/DIA ²
	ASARC ³							DA DCSINT ³
TTSP	ASARC/DAB ²			X	X	X	CBT DEV ⁴	DA DCSINT/DIA
	ASARC ³						MAT DEV ⁴	
Intelligence Report	DAB ²	X	X	X	X	X	DIA	Director, DIA ²
Validated Threat Statement	ASARC ³						DA DCSINT	DCSINT ³
ACQUISITION CATEGORY II REQUIREMENTS								
MNS	ASARC	X					CBT DEV—Threat Manager	DA DCSINT
ORD	ASARC		X	X	X	X	CBT DEV—Threat Manager	DA DCSINT
MIPS	ASARC		X	X	X	X	MAT DEV	DA DCSINT
AOA ¹	ASARC		X	X	X	X	CBT DEV	DA DCSINT
STAR	ASARC	X	X	X	X		CBT DEV—Threat Manager ²	DA DCSINT
							MAT DEV—Foreign Intel Off ³	
TEMP	ASARC		X	X	X	X	MAT DEV—Foreign Intel Off	DA DCSINT
TTSP	ASARC			X	X	X	CBT DEV ⁴	DA DCSINT
							MAT DEV ⁴	
Validated Threat Statement	ASARC	X	X	X	X	X	DA DCSINT	DCSINT
ACQUISITION CATEGORY III/IV REQUIREMENTS								
MNS	IPR	X					CBT DEV—Threat Manager	TRADOC DCSINT
ORD	IPR		X	X	X	X	CBT DEV—Threat Manager	TRADOC DCSINT
MIPS	IPR		X	X	X	X	MAT DEV	AMC
AOA ¹	IPR		X	X	X	X	CBT DEV	TRADOC
STAR	IPR	X	X	X	X		CBT DEV—Threat Manager ²	TRADOC DCSINT
							MAT DEV—Foreign Intel Off ³	AMC ³ DCSINT
TEMP	IPR		X	X	X	X	MAT DEV—Foreign Intel Off	TRADOC DCSINT
TTSP	IPR			X	X	X	CBT DEV ⁴	TRADOC ²
							MAT DEV ⁴	AMC ³
Validated Threat Statement	IPR	X	X	X	X	X	TRADOC ²	TRADOC ²

Table 1–1
Threat Support Responsibilities Matrix—Continued

Document	Type of review	Milestone					Threat prepared by	Threat approved/validated by
		O	I	II	III	IV		
							AMC ³	AMC ³

Notes:

¹ Approval/validation occurs early in AOA process—vice concurrencies to final, published COEA document. TRADOC DCSINT will review and approve threat portrayal AOA's when the primary support is provided by Threat Managers.

² Through MDR I.

³ Beyond MDR I.

⁴ CBT DEV (operational testing); MAT DEV (developmental testing).

Chapter 2

How To Obtain Intelligence

Section I

Obtaining Existing Intelligence Products and the Intelligence Dissemination Program

2–1. General

Department of Defense and non-DOD intelligence agencies publish a large volume of intelligence products and intelligence information reports on a wide range of topics of importance to the Army. The majority of the Army's intelligence requirements can be met in full or in part by existing published intelligence reports, or products to be produced if they are disseminated in a timely manner to agencies and commands with a valid requirement for the intelligence. The DOD Intelligence Dissemination Program links the requirements of the consumer with the efforts of the intelligence collection and production agencies within the framework of applicable security constraints. This section outlines the DOD, DIAR-59-1 and the Army Intelligence Dissemination Program and prescribes policies, responsibilities, procedures, and standards for implementation.

2–2. Intelligence Dissemination Program

a. The Intelligence Dissemination Program allows for an Army agency or command to register requirements for intelligence that will result in the automatic dissemination of recurring and non-recurring products within applicable security constraints. The program also allows for the one-time issue (secondary distribution) from stocks of previously issued publications. Army agencies and commands registering requirements for intelligence will be assigned a DIA intelligence dissemination customer account number.

b. Proper registration of an organization's intelligence requirements is key to obtaining the needed intelligence promptly. The identification of requirements for products is accomplished by selecting the subjects and geographic codes that support the organization's missions and functions. This information is processed by the DIA Customer Requirements Registration System (CRRS) program and this in turn becomes the organization's SII. The SII is incorporated into a DIA account and assures the automatic receipt of required products. The SII can and should be modified at anytime so the account accurately reflects changing mission requirements, or special situations. At a minimum it must be updated annually.

2–3. INSCOM

a. On behalf of DCSINT, HQDA INSCOM manages the DOD Intelligence Dissemination Program within the Army. Major duties include:

- (1) Establish and maintain files of Army organization mission statements and other pertinent documentation required to support validation.
- (2) Validate requests for all intelligence dissemination support from Army agencies and commands in CONUS and OCONUS not subordinate to a Unified Command.
- (3) Validate requests for the dissemination of SIGINT end product and current intelligence to all Army commands worldwide. This includes unified commands.
- (4) Assure the proper dissemination of intelligence products to DA Staff.
- (5) Represent and report to the DCSINT on intelligence dissemination matters throughout the intelligence community.
- (6) Evaluate and report to the DCSINT on the adequacy of the intelligence dissemination process.
- (7) Provide advice and assistance to Army elements on the intelligence dissemination process via the Customer Service Program (CSP).

b. Heads of the DA Staff will submit PRs in accordance with this regulation.

- c. The Commanding Generals of Army MACOMs are responsible for:
 - (1) Maintaining a SII program which supports missions and functions of the MACOM HQs and subordinate elements.
 - (2) Reviewing, validating, and submitting SIIs in accordance with this regulation only for those requests that cannot be fulfilled within the command agency.
- d. Strategic Military Intelligence Detachment (STRAT MID) Commanders supporting production centers are responsible for:
 - (1) Establishing and maintaining a SII account.
 - (2) Updating SII on an annual basis during two week annual training.
 - (3) Validating and forwarding SII through their supported production center.

2-4. Approval recommendations

A formal request constitutes the certificate and endorsement that the intelligence or intelligence information requested is essential for the command to accomplish its mission and that the command is authorized to receive, store, and handle the material as it is classified.

2-5. Establishing a DIA intelligence dissemination customer account

Defense Intelligence Agency is chartered by DOD Directive 5105.21 to supervise a DOD-wide intelligence dissemination program that provides centralized services in support of DOD. This entails maintaining a system (the DIA customer account) to disseminate intelligence. Army requests to establish a customer account and to register intelligence dissemination requirements are concurrent actions. To do this, take the following steps:

- a. Review the CRRS program at the MACOM and Major Subordinate Command (MSC) intelligence staff office. Familiarization training is available from the Senior Intelligence Officer (SIO).
- b. Complete the following mandatory data elements in CRRS:
 - (1) To establish a DIA account; complete the administrative data elements which generates the following:
 - (a) Account administrative data.
 - (b) Point of contacts (POC).
 - (c) Mission and Function Statement.
 - (2) Identify intelligence needs by completing the Intelligence Functional (IFC) and Intelligence Publications data elements which generates dissemination of the following type products:
 - (a) Recurring (hard copy).
 - (b) Non-recurring (hard copy).
 - (c) Electrically disseminated (Defense Message System (DMS)).
 - (d) Electronic (floppies, tapes, and so forth)
 - (e) On-line (future).
- c. Forward CRRS package or changes through command channels to the Commander, INSCOM, ATTN: IAOP.

2-6. Updating the SII, SIGINT end products (SEP) and current intelligence (CURINTEL) accounts

- a. Senior Intelligence Officer's will need to frequently review the requirements and supporting documentation to ensure that mission requirements are fully addressed. Modifications may be submitted at any time through command channels as deficiencies are identified.
- b. U.S. Army Intelligence and Security Command Dissemination Program Manager (DPM) will contact each SII account holder annually and SEP accounts semi-annually. Statement of Intelligence Interest accounts and the SEP accounts may be modified through INSCOM DPM SII Worksheet located on INTELINK under DPM Home Page URL: http://www.inscom.ic.gov/DA_DPM/customer_sii_update.htm or INTELINK-S http://www.inscom.army.smil.mil/DA_DPM/customer_sii_update.htm. Accounts may also be modified by contacting INSCOM DPM at their shared e-mail address: dadpm@inscom.ic.gov.

2-7. Obtaining secondary dissemination

Senior Intelligence Officer's of SII accounts can submit requests directly by using the DPM Secondary Dissemination Request located on INTELINK under INSCOM DPM Home Page, URL: http://www.inscom.ic.gov/DA_DPM/document_request_split_page_.htm or INTELINK-S http://www.inscom.army.smil.mil/DA_DPM/document_request_split_page_.htm or send customer requests electronically via e-mail to dadpm@inscom.ic.gov.

2-8. Obtaining human intelligence reporting

Intelligence Information Reports (IIRs) and IIR Enclosures are posted on INTELINK and INTELINK-S under the DIA Home Page or send customer request electronically via e-mail to: dadpm@inscom.ic.gov.

- a. To receive an IIR, agencies must be—
 - (1) Recognized participants in the worldwide indications and warning system.

- (2) Authorized and delegated producers of Army approved general or scientific and technical intelligence.
 - (3) Agencies designated to the intelligence collector through the tasking of an intelligence collection requirement.
 - (4) Agencies within the intelligence collector's chain of command.
 - (5) Agencies that in the judgment of the intelligence collector will be immediately and critically impacted upon by the receipt of a particular IIR.
 - (6) Agencies that can identify a lack of finished intelligence, and have an operational requirement for special categories, subjects, or geographical areas of information such as terrorism, narcotics activities, and the transfer of protected technologies.
- b.* Commands meeting the criteria in paragraph a above, and requiring secondary dissemination of IIRs will follow the request procedures listed in paragraph 2-7. As a minimum, the request must include the IIR number and subject.
 - c.* If the requester was on the approved distribution for the cover IIR request for enclosures go directly to DIA (S-03), Washington, DC 20340-3342. Email: DIWOHP@B3B1.B3+DIA-HIGGINS.DODIIS

2-9. Obtaining recurring electrically disseminated intelligence products

U.S. Army Intelligence and Security Command maintains the Army database that reflects DOD recurring electrically disseminated intelligence products. INSCOM's CURRINTEL system will be used by the customer to register initial requirements. A request to make changes to the Army data base for dissemination of intelligence products may be submitted by message through command channels for collateral to: DA AMHS WASHINGTON DC//DA DPM INSCOM-IAOP-OR-ITP// or for SCI DA IDHS//DA DPM INSCOM-IAOP-OR-ITP//. The mission and functions statement on file for your organization must support your request.

2-10. Obtaining SIGINT end product (SEP)

DIAR 59-1, User's Guide to Intelligence Dissemination/Reference Services, has delegated to the Army, INSCOM the authority to validate and process SEP requirements directly with the National Security Agency (NSA). This includes support for Army MACOMs and Army elements of Unified Commands. MACOMs will use CRRS to register initial requirements and follow the procedure in paragraph 10a for changes. Army MACOMs and Army elements of Unified Commands will follow procedures in paragraph a and b below for initial requirements and changes. INSCOM has posted SIGINT Customer account information on INTELINK under INSCOM DPM Home Page, URL: http://www.inscom.ic.gov/DA_DPM/document_request_split_page_.htm. On INTELINK-S use http://www.inscom.army.s-mil.mil/DA_DPM/document_request_split_page_.htm. SIGINT end product reports are issued by NSA based on information obtained from communications intelligence (COMINT), electronic intelligence (ELINT), and/or foreign instrumentation signals intelligence (FISINT). Dissemination is made to valid Army customers either as electrical messages or as hard copy documents. Requests for SIGINT end products must be submitted through command channels to INSCOM for validation and follow the guidelines below:

- a.* Request for SIGINT end product will be submitted via e-mail or through SSO channels. E-mail address is: dadpm@inscom.ic.gov and posted on INTELINK and INTELINK-S under INSCOM DA DPM Home Page. SCI message address: DA IDHS//DA DPM INSCOM-IAOP-OR-ITP//. Information addressees should be all echelons in the established command channel. Requests should not be sent directly to NSA. NSA will not honor requests that have not been validated by INSCOM.
- b.* Changes to requirements for SEP can be made at any time to accommodate mission changes or special requirements and should be submitted following the procedures in a above. Frequent requirement changes should be the basis for reevaluation of any organization's basic dissemination program.

2-11. Requesting approved intelligence product distribution lists

Department of the Army Staff, MACOMs and MSCs that produce scheduled and unscheduled finished intelligence will request an Army approved distribution list through INSCOM. Requests for distribution lists will be forwarded to INSCOM, via e-mail no than later 30 working days prior to publication data using Community On-line Intelligence System End User Manager (COLISEUM). Requests will follow the guidelines below:

- a. Hard copy.*
 - (1) General Military Intelligence producers will submit a request to DAMI-FI for a distribution list no later than 30 working days prior to publication data using COLISEUM.
 - (2) Scientific and Technical Intelligence producers will submit information via COLISEUM directly to DIA for a distribution list 30 working days prior to publication and provide a copy furnished to DAMI-FI.
- b. Electrical.* All Army Intelligence producers will submit information via COLISEUM to DAMI-FI within 15 working days prior to the electrical release of the product.
- c. Electronic (Floppies, Tapes, and so forth).* All Army Intelligence producers will submit a request to DAMI-FI for a distribution list 15 working days prior to publication date using COLISEUM.

Section II

Obtaining New Intelligence Production

2-12. The production requirement process peacetime

The Army process for obtaining intelligence products conforms to the DODIPP. The key objective of the DODIPP is to satisfy the customer by sharing intelligence resources, eliminating duplication, maintaining quality, encouraging widest dissemination, exploiting electronic technology, and improving efficiency and timeliness. DODIPP is implemented through a shared production program that makes the expert available to all customers by logically dividing production responsibilities, assigns each requirement to a primary production center based on major topics, sets procedures, policies and standards and represents a managed response to intelligence requirements. This chapter specifies procedures for generating, validating, assigning, and responding to PRs. The capstone document Department of Defense Intelligence Production Program (U), DOD-0000-151-94 describes the policy, principles and concepts for the decentralized execution of DOD production. The COLISEUM was developed by DIA to support DODIPP with an on-line, automated requirement management capability for research, development submission and review, validation, and assignment of information requirements.

a. All Army organizations governed by this regulation have a supporting intelligence office. The supporting intelligence office might be a single intelligence officer (military or civilian), a small office, or a self-contained intelligence organization. This regulation does not require or authorize creation of new intelligence positions to support customers.

b. Each Army MACOM designates the supporting intelligence office(s) that will prepare PR for customers subordinate to the MACOM.

(1) The supporting intelligence office as defined in DODIPP, serving the Army Staff is HQ, INSCOM, ATTN: IAOP.

(2) A supporting intelligence office takes the customer's questions and tries to answer them using locally available knowledge and Department of Defense Intelligence Production Community (DODIPC) intelligence products. If local intelligence holdings do not suffice, the supporting intelligence office prepares a PR utilizing the DIA COLISEUM system per figure 2-3.

(3) Until the DODIPP relational database software, COLISEUM becomes generally available to the DODIC, the Army validation office will use the Army Requirements Management System (ARMS) for preparation of PRs. Preparation of PRs is accomplished by the supporting intelligence offices using their existing word processing system.

(4) A PR is not complete unless it contains, as a minimum, the data required in figure 2-2 and the APIN(s) associated with the requirement. The supporting intelligence office transmits the completed PR by electronic means whenever possible. Timeliness in the transmission of PRs is critical. The Army validation office (VO) will accept PRs only on floppy disk or by e-mail. In rare instances when automation equipment is not available and the supporting intelligence office transmits a hard copy, a memoranda of transmittal is not required.

c. Each MACOM establishes its internal chain to review PRs. To be valid, a PR must be complete, pertinent to the mission of the customer, and not duplicating an existing PR from the same MACOM.

(1) The MACOM reviewing office will annotate its organization and POC data after that of the supporting intelligence office under Item 10 of the PR.

(2) When transmitting a PR as an electronic file via floppy disk or e-mail, the MACOM reviewer will add the POC and date of review following the organization data under item 10.

(3) Ultimately, Army chains of command will prepare and transmit PRs using relational database software which creates a PR record consisting of text, date, numeric, and memo fields. On such software, each "through addressee" for a PR will have its own fields to document and date its review action.

d. The DODIPP requires each unified command and service to designate a VO. The VO is the final office responsible for reviewing and validating PRs. The VO is the sole production validation entity.

(1) HQ INSCOM, IAOP is the VO for all Army organizations governed by this regulation. Organizational data for the Army VO is listed under item 11 of the PR.

(2) The Army VO after validating a PR, assigns the PR to the DODIPC Production Center responsible for the topic(s) and countries specified in the PR. The HQDA, VO bases the PR assignment on the DODIPC production responsibilities per the DODIPP IFC.

(3) The Army VO will complete items 12 thru 21 of the PR.

(4) Electronic PR records prepared on relational database software will have specific text fields for use by the Army, VO to assign the PR to a primary production center, and additional text address fields to send information copies of the PR record to the NMIPC, Directorate of Operations, and to the customer.

(5) The Army VO assigns a PR for action to a primary production center and simultaneously provides information copies of the assigned PR to possible collaborative production centers, and to the NMIPC, Directorate of Operations. The Army VO will provide copies of assigned PRs to MACOMs and the original supporting intelligence office that prepared the PR not less than quarterly.

(6) The Army VO will maintain a current database of the PRs it has received and acted on. This database will be

available to the NMIPC, Directorate of Operations, to the headquarters of every Army MACOM, and to every production center assigned a PR by DAMI-FI during the reporting month.

(7) Ultimately, COLISEUM software used to prepare, transmit, and assign PRs will allow the NMIPC, Director of Operations, the Army VO, the NGIC, each Army MACOM headquarters, and eventually the supporting intelligence offices of each customer to format a report from the dynamic data fields in the database. All concerned Army offices will be able to query the database and select the data fields each needs to build management reports.

(8) Until, COLISEUM becomes generally available to the DODIPC, the Army VO will use the ARMS and electronic connectivity to the NMIPC, the NGIC, and Army MACOM headquarters to record, transmit, account for, and report on all PRs validated and assigned.

(9) As a primary production center, the NGIC receives PRs assigned by VOs and responds to them by preparing an official production center response (PCR) utilizing the DIA COLISEUM system. First and foremost, the PCR is to reply to the customer(s) by responding to their supporting intelligence office-the generator of the PR(s). The PCR also notifies the DODIPC of what product will satisfy the customer(s) PRs, when, how, and by whom.

(a) The NGIC must transmit the PCR as soon as possible after receipt in order to meet short product suspense's, but not later than 20 working days for any scheduled product. For PCR that are a response to a CIC, the response must be transmitted when there is evidence to suggest that the CIC was breached. A complete PCR contains all data specified in accordance with Appendix C, DODIPP policy document. A primary production center is authorized to provide additional detail and information within its production center response as it deems necessary.

(b) Just as with PRs, NGIC PCRs are electronic files.

(c) The principal addressee for a PCR will always be the supporting intelligence office(s) which represent the customer(s) by preparing the PR(s). Information copies of the PCR go to the MACOM VO and the Army VO that assigned the PR(s), the NMIPC, Directorate of Operations, and all collaborative production centers listed in the PCR.

(d) Supporting intelligence offices are responsible for notifying their chain of command when a PCR to their PR has been received.

(e) Using the DODIPP relational database software COLISEUM and wide-area network, a PCR will be an electronic data record containing text, date, numeric, and memo fields. In ARMS, a PCR record and a PR record are linked using the PR control number and product number unique to each.

(f) The PCR is the management record and tool used by Army and throughout the DODIPC to document all production. The PCR promises a product to all corresponding customers with valid, assigned PRs. PCRs are the data records which permit primary production centers to schedule work internally, assign collaborative work to collaborating production centers, and keep VOs and the NMIPC Directorate of Operations informed of production planned and accomplished.

(g) The unique product number which first appears on a PCR will later appear, unchanged, on the product itself.

(h) Primary production centers will periodically have to update a PCR for a variety of reasons. Some of the most common reasons include: adding a new PR which has additional germane questions, changing the projected date for dissemination of the product, or adding/changing the listing of collaborative production centers and their input.

(i) Each update of a PCR will carry the original product NUMBER. Updated PCR will be clearly recognizable throughout the DODIPC by the date on the PCR, additions/deletions to the paragraph listing PR Control Numbers, additions/deletions to the list of collaborative production centers and their input.

Peacetime

Customer states mission	Supporting Intelligence Office	Validation Office-validates	Primary production center
driven intelligence needs to Supporting Intelligence Office (TSO).	assists in fulfilling the customers requirements and if necessary creates a production request (PR).	assigns the requirement a primary production center.	produces a product which is responsive to the customer.

Figure 2-1. The Requirements Process Peacetime

Crisis/War

The crisis/engaged	To	The Unified Command Validation	Which	Respond or assigns
Joint Task Force states its needs.		Office responds or forwards the request to the National Military Joint Intelligence Center (NMJIC).		the production request to the production center for completion.

Figure 2-2. The Requirement Process Crisis/War

2-13. Guidance to customers when preparing production requirements

a. The PR number is intended to be unique throughout the DODIPC to serve as the sole reference number for a PR from inception until cancellation. Each Validation Office will have a relatively fixed number of customers.

b. The PR subject serves also as the PR title. This is one of the key “text” fields searched by relational databases when reporting on the status of PRs. Strive to include as many key-words in this item as possible.

c. The specifics of each customer organization will vary. Item 3 captures the actual customer organization that has intelligence questions as opposed to the supporting intelligence office that prepared the PR. An example of a customer organization might be:

Commander, U.S. Army Communications and Electronics Command
ATTN: Program Manager-SINGARS
Ft. Monmouth, NJ 12345
MESSAGE ADDRESS: CDRCECOM FT MONMONTH NJ//AMSEL-PM-S//
e-mail: singars@monnj.com
FAX: DSN: 123-4567
Contact: POC name, Commercial (212) 343-4545, DSN 123-4545

d. The date of the PR is the date the supporting intelligence office completes the PR.

e. The best estimate by the customer of the latest date on which the intelligence required will be of value. The customer and its supporting intelligence office must be knowledgeable of the total time needed by their chain of command to review and transmit the PR. Item 5 will be a key factor used by the production center in determining how to respond and how much effort to expend on the PR. The date (YYMMDD) entered in item 5 must be explained in the Statement of Requirement.

f. The customer and its supporting intelligence office must make every effort to reduce contradiction and confusion when specifying form and frequency of response.

(1) State the one best media, then list a second and third acceptable alternative. If a product is needed on electronic media (floppy disk, on-line access, and so forth), specify the computer hardware/software which will receive and use the electronic product. Fully justify any request for color.

(2) State only one frequency choice; elaborate on the reasons behind that choice in the Statement of Requirement. Remember, all customers will review their PRs annually. Biennial and Triennial products will undergo multiple PR reviews between editions. No product will be automatically updated on a fixed schedule.

(3) If the PR is intended to expand on an existing product or one that is in preparation, list the product number and title. Be as precise as possible-specify addition of a chapter or appendix, or list which existing chapters, appendixes, figures, or tables need expansion or refocus.

(4) Stipulate the highest level of classification at which the product is usable. Specify if contractors will need access to the product in whole or in part.

(5) This item should consist of at least one text paragraph. The first paragraph must be a summary/abstract/precis of the requirement in 50 words or less. For ad hoc production, this paragraph is the minimum acceptable input for this item. This first paragraph should not include any information that is in the subject unless absolutely necessary for clarity. It should include the topic, names the program or mission supported, and indication of level of detail required. If time permits, or the complexity of the PR makes it necessary, subsequent paragraphs can provide any justification for the requirement, detailed questions on sub-portions of the requirement, and provide priorities on multiple countries, topics requested. The second (and all subsequent) sub-paragraphs should list the questions.

g. This is another “text” field permitting elaboration and comment if needed. Specify any PRs being superseded. Specify a primary APIN number and other applicable APINs.

h. Strive for the lowest classification possible for the contents of the PR. Classified documents attached to the PR

should be clearly marked and distinguished from the PR itself. Send SCI PRs and SCI enclosures to PRs through SCI channels.

i. Item 10 lists the supporting intelligence office that prepared the PR. An example of a supporting intelligence office might be:

Commander, U.S. Army Communications and Electronics Command
ATTN: Foreign Intelligence Office (AMSEL-MI-I)
Ft. Monmouth, NJ 07703-5000
MESSAGE ADDRESS: CDRCECOM FT MONMONTH NJ//AMSEL-MI-I//
E-mail: intel@monnj.com
FAX: DSN: 123-4567
Contact: POC name, Commercial (212) 343-2323, DSN 123-2323

j. Each unified command, each Service, and DIA has a VO. The VO is the validating authority for the PR, and is the office authorized to assign the PR to a primary production center. The VO for Army is:

Headquarters INSCOM, ATTN: NAOP-OR-ITP
8825 Beulah Street
Ft. Belvoir, VA 22060-5246
E-mail: dodiis is jadress@inscom.ic.gov
collateral jadress@inscom.army.smil.mil
unclas jadress@vulcan.belvoir.army.mil

ITEM 1 - PR NUMBER: A 12-space number having ten characters. The first four characters are the customer's SII account number; DC can be used until an SII account is established. The second two numbers are the fiscal year. The last four numbers are the customer's sequence number for PRs submitted in the fiscal year (for example, C610-94-0001).

ITEM 2 - SUBJECT: A short descriptive title, UNCLASSIFIED whenever possible.

ITEM 3 - CUSTOMER'S ORGANIZATION: POC, organization, mailing, message, e-mail, and FAX address, commercial and DSN numbers (including FAX) of the customer.

ITEM 4 - DATE OF PRODUCTION REQUIREMENT: (YYMMDD)

ITEM 5 - DATE PRODUCT REQUIRED: (YYMMDD)

ITEM 6 - FORM AND FREQUENCY OF RESPONSE:

a. Media of product (message, memorandum/letter, floppy disk, on-line data base, database printout, bound hard copy report/study/handbook, and so forth)

b. Frequency (one-time, as required, recurring.) All ad hoc PRs are treated as one-time PRs. For recurring PRs, specify periodicity.

c. Revision of existing product or new product.

d. Classification and releasability of product.

ITEM 7 - STATEMENT OF REQUIREMENT: Provide a summary of the requirement in 50 words or less in the first paragraph. Provide additional information in succeeding paragraphs. Prioritize the questions to be answered by the product.

Figure 2-3. Production Requirements

Prioritize all lists of countries, lists of critical technologies, and separate questions. If multiple countries/technologies carry the same priority, list these by time-urgency. Specify frequency of producer feedback to customer during the production phase.

ITEM 8 - COMMENTS: Available for any additional comments necessary. Specify what PR(s), if any, are being superseded by this PR. Specify primary Army Priority Intelligence Need (APIN); list other applicable APINs.

ITEM 9 - SECURITY CLASSIFICATION: The highest classification of the questions and information contained in the PR.

ITEM 10 - SUPPORTING INTELLIGENCE OFFICE: POC, organization, mailing, electrical message, E-mail, and FAX address, commercial and DSN numbers (including FAX).

ITEM 11 - VALIDATION OFFICE:

Headquarters INSCOM, ATTN: NAOP-OR-ITP

8825 Beulah FT Belvoir, VA 22060-5246

E-MAIL: jadress@inscom.ic.gov

jadress@vulcan.belvoir.army.mil

jadress@inscom.army.smil.mil

FAX (UNCLAS): DSN 235-1011

Contact: Commercial (703) 706-2278, DSN 235-2278

ITEM 12 - PRIMARY IFC: VO enters the one most descriptive intelligence functional code for the complete PR.

Figure 2-3. Production Requirements--Continued

ITEM 13 - OTHER IFCs: VO may enter other discrete IFCs that can be clearly defined within the PR.

ITEM 14 - PRIMARY AOR CODE: VO enters the AOR most covered within the PR or 'worldwide' if appropriate.

ITEM 15 - OTHER AOR CODES: VO enters up to two additional codes if appropriate.

ITEM 16 - PRIMARY COUNTRY CODE: VO enters the one country most discussed in the PR.

ITEM 17 - OTHER COUNTRY CODES: VO enters other countries requested in the PR.

ITEM 18 - PRIMARY PRODUCTION CENTER ASSIGNED: Using the primary IFC and region information entered above, the VO specifies the primary production center to which the VO assigns the PR.

ITEM 19 - POSSIBLE COLLABORATIVE PRODUCTION CENTERS: Using the other IFCs and region information entered above, the VO determines possible collaborative production centers.

ITEM 20 - DATE OF VO ASSIGNMENT: YYMMDD

ITEM 21 - DATE OF CUSTOMER RECERTIFICATION: Customer enters YYMMDD following annual review of the PR. Annual review takes place during the twelfth month following validation. This date will be updated annually for as long as the customer determines that the content of Item 7 'Statement of Requirement' remains unchanged and reflects the customer's intelligence need.

Figure 2-3. Production Requirements--Continued

2-14. Guidance when preparing a production center response

a. The primary production center lists the PR Number of each PR addressed by the PCR and updates the PCR when a PR is added through assignment from a VO, closed out by the VO, or deleted through cancellation by a customer.

b. When a PR is narrowly focused and answerable in a concise, comprehensive product, the primary production center should strive to directly match product to PR. A first step would be the match the subject of the PCR, and the title of the product to the subject of the PR.

(1) When the primary production center determines that the best means to respond to a new PR is to add its questions to work on-going on a previously scheduled product, the primary production center should reissue the existing PCR after updating it to reflect addition of the new PR. The original PCR subject should not change.

(2) If a primary production center drafts a PCR to respond to multiple PRs, the PCR should carry a subject which applies to all the PRs.

c. The primary production center lists the production priority for the topic(s) and countries covered by the product. This priority is in accordance with the DODIPP production priorities in effect at the time the PCR is prepared. These production priorities are applicable throughout the DODIC. DODIPP production priorities can change throughout the

production process based on changes approved by the Defense Intelligence Production Center (DIPC) and the Military Intelligence Board (MIB). Change in DODIPP production priority necessitate an update to the PCR.

d. When the PCR is a one-for-one response to a PR, the product abstract can be a close transliteration of ITEM 7 “Statement of Requirement” of the PR. In all other instances, the primary production center crafts a product abstract not to exceed 50 words. The product number is the reference number for both the PCR and the eventual product. The primary production center must state why it cannot meet the form and frequency of product specified by the PR(s)-if this is the case.

e. Consists of a series of subparagraphs each of which lists a specific collaborative production center followed by a brief summary of what intelligence that collaborative production center will provide to the product. The contents of paragraph i below, can only be completed after the primary production center has coordinated directly with each collaborative production center.

f. Strive to make the PCR itself UNCLASSIFIED.

g. Extract VO data from the PR(s).

h. A primary production center will normally list its operations office POC and analytical POC here.

i. Completion of this paragraph by the primary production center is optional. The primary production center can coordinate between customer, supporting intelligence office, and production analysts here.

The NGIC, when acting as a primary production center, responds to an assigned PR by transmitting a PCR prepared as follows:

ITEM 1 - PR NUMBER(S): List the control numbers for all PRs covered by the product. The NGIC reissues an updated PCR every time the list of PRs change.

ITEM 2 - SUBJECT: For a single PR, use the PR subject verbatim. If the PCR adds a PR to an existing product, use the existing product's long title. If the PCR is to multiple PRs, create a subject for the PCR that encompasses the subjects of all the PRs.

ITEM 3 - PRODUCT PRIORITY: (Derived from DODIPP production priorities). COLISEUM will automatically assign priority.

PARA 3 - PRODUCT SHORT TITLE: The product short title must include the NGIC's primary production center code, reference DODIPP number, unique sequence number, and current fiscal year (YY).

ITEM 4 - PRODUCT(S) Provide subject, abstract, product media, frequency, target dissemination date, target audience, classification and releasability, product number, AOR, country(ies), and DODIPP record ID code.

ITEM 5 - COLLABORATIVE PRODUCTION CENTER(S): List all collaborative Production Centers; what and when each will contribute.

ITEM 6 PCR CLASSIFICATION: Wherever possible, the PCR should be UNCLASSIFIED.

ITEM 7. VO: The assigning VO.

ITEM 8. Production POC: Provide full POC and organizational data.

ITEM 9 - PRIMARY PRODUCTION CENTER COMMENTS: (Optional)

Figure 2-4. Production Center Response

Chapter 3

Threat Intelligence Support

Section I

Threat Intelligence Support Programs

3-1. General

a. The purpose of threat intelligence support programs is to ensure that force, concepts, doctrine, training, organization, technology, and materiel systems the Army is developing for the 21st century can effectively and efficiently

respond to an evolving global threat environment. To achieve this purpose, threat intelligence support must be timely, consistent, and continuous.

(1) Timeliness ensures that threat considerations are provided to combat and materiel developers throughout all phases of the combat and materiel development cycle in order to properly influence the requirement for and development of force, concepts, doctrine, training, organization, technology, and materiel systems.

(2) Consistency requires that multiple users including those engaged in simulator and target development, modeling and simulation and threat scenario development work from a standard, approved intelligence baseline.

(3) Continuous threat support means that the impact of the threat is considered throughout the life cycle of a materiel system, from identification of a deficiency, through and including post-development product improvements and horizontal technology integration. It ensures that organizational and doctrinal developments are supported throughout their conceptual phases and after implementation.

b. A threat intelligence support program consists of the following:

(1) Department of Defense (DOD), national intelligence community, and Army intelligence products (documents, data bases, models, simulations, concepts, and scenarios).

(2) The procedure designed to respond to intelligence requirements that are not fulfilled by published intelligence products.

(3) Procedures used to apply threat data in a study, analyses, or simulation, or to integrate threat into the planning and execution of a developmental or operational test.

c. Threat intelligence support programs will be initiated early in the combat development process. Early intelligence support ensures that the impact of the threat is considered and applied during the entire acquisition process, which may lead to the identification of a requirement for a specific materiel system or a change in organization, doctrine, or training. (Figs 3-1, 3-2, 3-3 and 3-4 depict threat support activities throughout a program's life-cycle.)

d. Threat support programs will be initiated to support the development of all force, combat, and materiel development programs and studies.

e. At the start of a study or project, the proponent will identify threat intelligence support requirements. The threat intelligence support activity at each command level is responsible for 1) coordinating and providing threat support to combat and materiel developers; and 2) for the application of the threat in support of programs and studies conducted within the command. An ICT may be formed to develop requirements for an acquisition program. A threat representative, usually from the proponent activity, will participate in the ICT to identify threat support requirements.

f. The relationship between a U.S. system or program and the specific threat is dynamic and reflects changes in tactics, doctrine, and technological advancements. The threat support activity of proponent commands will maintain a life cycle threat audit trail for each program.

g. The basis or start point for developing the threat in support of a specific program, system, or study is threat data sources, to include a variety of DOD threat databases maintained as part of the DODIPP. As part of the Threat Coordinating Group, the ODCSINT TISO will coordinate and assist in ensuring threat support for the development process.

h. Specific guidance for the preparation of threat assessments is contained in appendix B.

3-2. Intelligence products

Intelligence products are publications, automated databases, signatures, object oriented simulations, and electronic media that address foreign force capabilities in the near term (0-5 years), mid-term (5-10 years) and far term (10-20 years). Products from DODIPP production elements will be used in developing threat assessments for satisfying system-specific threat support requirements. To ensure consistency throughout the Army intelligence and development communities, for each battlefield operating system (BOS), ODCSINT (TISOs) will publish an annual listing of suggested baseline intelligence products that should be included in the STAR bibliography. The bibliography is not intended to be all inclusive; in the absence of DOD Intelligence Production Program (DODIPP) products, users are not restricted from examination of other sources that may answer threat support requirements for specific programs or systems. These baseline products are essential for sustaining the provision of consistent threat throughout the study and acquisition process, and represent the start point for assessments prior to initiating specific requests for support.

3-3. Threat intelligence in modeling and simulation

a. The Army M&S Master Plan establishes three M&S domains: Training, Exercises, and Military Operations (TEMO); Advanced Concepts and Requirements (ACR); and Research, Development and Acquisition (RDA). Multi-discipline Intelligence support is required for M&S in each of these domains.

b. Simulation users will work closely with their supporting intelligence offices to ensure that threat data and representations used in simulations are current, accurate, and validated. Models & simulations (M&S) that are used for test and evaluation, education and training, research and development, or production and logistics will be responsive to the provisions of AR 5-11, in addition to the provisions in this regulation. This also includes semi-automated forces (or computer generated forces), or M&S that operate in a distributed interactive simulation (DIS) environment. TCGs and existing validated databases will be used to satisfy the requirement for current and accurate data inputs. All developers,

testers and trainers will access intelligence databases through their supporting intelligence officer. Problem areas and events that cannot be portrayed accurately will be fully documented for decision through the chain of command. Deviations from validated scenarios and threat data will be forwarded to ODCSINT for approval through intelligence channels. Problems and deviations will be identified at each MDR meeting or in process review meeting for consideration by study members. Documentation will include, as a minimum, assumptions, decision rules, uses, limitations, data requirements, and data currently stored.

c. DOD regulation 5000.2-R requires each threat representation subject to validation procedures to establish and document a baseline comparison with its associated threat and to determine the extent of the operational and technical performance differences between the two throughout the life cycle of the threat representation.

3-4. Threat simulators and targets

a. Threat simulators provide physical representations of threat systems for use in developmental testing, operational testing and training. A threat simulator exhibits one or more operational characteristics/physical signatures of an actual threat system. Threat simulators used in testing that supports a system MDR must be validated and accredited. Validation is the process used to identify, document, and analyze the differences between a threat system and the system it represents. Accreditation is the process of determining the extent to which the simulator or target supports the requirements of the specific test or evaluation. When actual threat systems are used, the accuracy of their parametric data must be certified and any limitations imposed by instrumentation noted.

b. Threat systems used to support T&E are subject to a process that identifies, analyzes, and documents the differences between the representative threat and the DIA approved intelligence assessment of the actual threat system. When actual threat systems are used, they are certified to the accuracy of their parametric data and limitations imposed by instrumentation are noted.

3-5. Threat scenario development

a. Army analytic, training, testing and research agencies require basic guidelines regarding precursory events, time lines, and threat employment concepts, in addition to data on threat force structure and weapon systems characteristics. This family of threat scenarios contains current Defense Planning Guidance (DPG) Illustrative Planning Scenarios (IPS) as well as other threat scenarios based on Service input to the Threat Assessment Scenario Committee (TASC). The scenario development process is shown in figure 3-4.

b. To achieve accuracy, commonality, and consistency of the threat in scenarios, the following guidelines apply to the development of threat force scenarios:

(1) The DPG IPS provides the services with a plan for development of necessary military capabilities to maintain the Nation's security. They will be used to begin development of scenarios intended to support force and materiel development processes. The DPG IPS contains planning scenarios intended to:

(a) Provide a general illustrative sequence of events on which to base force development planning for the future 20-year time frame and to assess risk to programmed forces.

(b) Provide a common set of U.S. friendly force assumptions for use by the Services in computing readiness, sustainability, mobility, and modernization of resources.

(2) ODCSINT (FI) will review the DPG IPS assumptions for impact on threat and provide scenario development input to the TASC. To assist DAMI-FI in this task, TISOs will provide DAMI-FI input on scenario areas of concern based on the execution of the scenarios in their respective acquisition programs.

(a) National Ground Intelligence Center (NGIC). NGIC will develop threat ground operational concepts for the scenarios in the DPG IPS on which TRADOC will base the TRADOC standard scenarios.

(b) U.S. Army Training and Doctrine Command (TRADOC). TRADOC standard scenarios (high and low resolution) will be used in studies for analyses to identify Army force modernization needs encompassing doctrine, organization, training, leadership, and materiel. Threat scenarios developed by TRADOC and approved/validated by ODCSINT and/or DIA through the TCG process will serve as the base for Army combat and materiel development studies, unless otherwise directed by DA. TRADOC will use the threat operational concepts developed by NGIC and threat data derived from DODIPP sources to develop standard scenarios. Data derived from other sources will be highlighted and submitted for approval through the TCG. Army schools, centers and activities involved in force and materiel development will use these approved scenarios for analyses. If threat excursions are employed, they will be highlighted clearly in study reports.

(c) Concepts Analysis Agency (CAA). ODCSINT guidance to CAA on global force employment scenarios will be based on specific study and model requirements. Generally, the NGIC-developed threat operational concepts will serve as the start point for scenario development to provide a common threat basis for annual planning and programming studies conducted for the ARSTAF. ODCSINT (DAMI-FI) will convene TCGs as needed to review results of analyses and to ensure that intelligence data on threat doctrine and force employment are logical and consistent.

3-6. Threat Integration Staff Officer (TISO)

a. A TISO is designated to function as the HQDA threat integrator for designated mission areas, programs and/or

materiel systems. The TISO represents ODCSINT on all aspects of threat support throughout the life cycle or study process. The TISO system complements the ODCSOPS system integrator, Assistant Secretary of the Army (Research Development and Acquisition) (ASA (RDA)) staff officer, and the PEO representative, and is designed to foster close coordination among the intelligence community and MACOMs, PEOs, and ARSTAF agencies to ensure the timely integration of threat into technology programs and the materiel development and acquisition process. The TISO system supplements existing management procedures but does not relieve ARSTAF agencies, PEO/PMs and MACOMs of established responsibilities.

b. Duties of the TISO are:

- (1) Represent the DCSINT and serve as primary HQDA staff point-of-contact for threat integration.
 - (2) Coordinate implementation of Army policy relating to threat support.
 - (3) Establish and manage TCGs for ACAT I and II systems, major automated information systems, POM-related studies, and selected DA studies and analyses.
 - (4) Provide timely DA threat guidance to threat support activities and commands responsible for technology, combat, materiel, simulator, simulation, and target development.
 - (5) Coordinate HQDA approval for all threat assessments, system threat assessments, and STARs, written or oral, to support ACAT I and II systems and selected studies, computer models, and analyses.
 - (6) Coordinate DIA validation of threat assessments written to support systems requiring DAB decision review.
 - (7) Direct the threat support process to ensure timely and consistent application of MDI to ACAT I and II systems (DODD 5000.1), Class I-III information systems (DOD 5000.1), and selected studies and analyses.
 - (8) Review and approve CICs that impact on the effectiveness, survivability, or security of the U.S. system. Review PRs that support CICs.
 - (9) Coordinate appropriate ODCSINT participation in STFs and SSGs for MACOM-managed studies.
 - (10) Coordinate with DOD, DIA, and other Service intelligence agencies on all aspects of threat intelligence support to Army-specific or joint Service acquisition programs. Attends other Service threat steering group (TSG) meetings and serves as the DCSINT representative for Army approval of threat in other service STARs .
 - (11) Review threat statements and assessments contained in ARSTAF requirements, decision, and program documents in coordination with ODCSOPS and ASA (RDA).
 - (12) Represent ODCSINT on all ACAT I, II, and selected OSD T&E oversight system TEIPTs to ensure timely threat intelligence support. Support the TIWG chairman through his respective TRADOC TM and AMC FIO in order to assist in generating and articulating requirements for threat intelligence support.
 - (13) Approve and monitor use of threat data, when appropriate, during developmental and operational test and evaluation phases of the materiel development cycle for ACAT I and II systems, to ensure maximum benefit from knowledge of the threat environment.
 - (14) Recommend, as appropriate, the establishment of MACOM-chaired TCGs.
 - (15) Represent HQDA at MACOM-level TCGs, if requested and appropriate.
 - (16) Attend formal and informal program reviews in the course of the materiel life cycle, and determine impact of threat considerations on the progress of systems development.
 - (17) Ensure a smooth transition for STAR responsibility to AMC after MDR I approval, for ACAT I and II systems
 - (18) Provide threat intelligence support for ACTDs, ATDs, red team, and horizontal technology integration efforts.
- c.* ODCSINT is the approving authority for either establishing or ending TISO monitoring of systems. Generally, all programs designated as ACAT I or II systems and Class I-III automated information systems will be assigned a TISO. Other systems and programs will be assigned TISO monitoring on an "as required" basis with ODCSINT approval.

3-7. System Threat Analyst responsibilities (DAMI-FIT)

- a.* Provide threat and foreign scientific and technical (S&T) Intelligence information to the Army staff.
- b.* Coordinate threat support to Army technology based efforts.
- c.* Provide S&T threat support to the TRADOC Battle labs.
- d.* Assist combat and material developers in articulating foreign S&T requirements and facilitating the resolution of these requirements.
- e.* Monitor system critical intelligence parameters (CICs) and essential program elements, technologies, or systems, and assist cognizant intelligent analyst in determining when a breach is imminent.
- f.* Monitor international involvement in the research and development (R&D) process, and determine the degree to which international involvement may induce or reveal vulnerabilities in Army systems.
- g.* Work with the Army Science Board, Army Material Command, and the Ground Weapons Intelligence Security Support Council (GWISSC) and other boards as required, to identify key technologies that could lead to significant military capabilities, and develop a methodology, in conjunction with other Army and DOD organizations, that will protect any vulnerabilities that may be inherent in those technologies.
- h.* Provide scientific and technical analysis and support to the TISO's during the preparation and review of STARs.

3-8. Threat coordinating groups (TCGs)

a. TCGs are integrating bodies composed of the Army's combat and materiel development activities, test and evaluation organizations, and the intelligence community to coordinate the provision of timely, consistent, and approved threat intelligence support for technology efforts, throughout an acquisition life cycle, or a study process. The TCG work includes the identification, approval, and validation of threat intelligence support for a multitude of efforts.

b. The three major types of TCGs: technology, system specific, and mission areas are discussed below:

(1) Technology TCGs coordinate threat support requirements for ATDs and ACTDs. ACTD TCGs will be conducted at HQDA level and ATDs TCGs at the MACOM level with HQDA, ODCSINT participation. Additionally, other technology TCGs can be conducted either at HQDA or the MACOM level and may address the threats and vulnerabilities to other technology efforts such as emerging technologies or technology that may be used for HTI efforts.

(2) System specific TCGs coordinate threat support requirements for specific programs. For each ACAT I and II system, ODCSINT normally will establish and chair a TCG. Other programs of particular DA interest also may require a HQDA-level TCG. MACOMs will establish TCGs for ACAT III and IV programs as required.

(3) Mission area TCGs coordinate threat support requirements common to all systems within a given mission area. Mission area TCGs can be conducted either at HQDA or MACOM level.

c. The TCG chairman will coordinate the approval of threat assessments that are based on intelligence data provided in response to user requirements, and will keep the Army leadership informed of the threat.

d. For new programs, system-specific TCGs will be formed immediately following an MDR 0 decision to continue program development.

e. Membership of each HQDA managed TCG will consist of representatives from the Army staff, combat and materiel development commands, MACOMs, test and evaluation organizations, and the Army intelligence community as appropriate. Additionally, representatives from DIA and other Services may be invited to take part in TCGs.

f. Functions of system specific and mission area TCGs are to:

(1) Assist combat and materiel developers in articulating their intelligence requirements and facilitating the resolution of issues related to the threat.

(2) Develop, for the user, a comprehensive baseline of intelligence products from appropriate approved intelligence documents. Ensure that the user considers all-source intelligence data.

(3) Coordinate and review combat and materiel developers' CICs and ensure the development of PRs in response to identified CICs.

(4) Review intelligence data and threat portrayed in the concept formulation process and provide recommendations to appropriate agencies.

(5) Coordinate review of models, scenarios, and analyses for correct application and interpretation of threat.

(6) Coordinate and review the Land Threat Environment Projections (LTEP) and new threat products such as those related to Information Warfare (IW) and Command and Control Warfare (C2W).

(7) Coordinate and review threat support for developmental and operational testing, to include use of scenarios, simulators, simulations, surrogates, and targets.

(8) Coordinate the review of the STAR, TTSP, and threat portions of program management documents, such as MNS, ORD, MIPS, AOAs and TEMPs.

(9) Provide for transition of threat intelligence support from the generic mission area to appropriate TCGs established to support ACAT I and II systems.

(10) Identify threat and threat intelligence support issues and determine responsibility for resolution.

3-9. Threat assessments

a. The proponent responsible for developing specific program documents such as a MNS, ORD, or TEMP that requires a written threat assessment for that document is outlined in Table 1-1. The threat assessment will provide a summary of current and projected threat, targets, and missions of the proposed systems emphasizing the interactive effects of the system and threat.

b. When drafting threat assessments, the supporting intelligence office will use DODIPP data sources. If DODIPP sources are not available, other source data will be highlighted and submitted for approval through intelligence channels for use in threat assessments.

c. The appropriate MACOM headquarters is responsible for coordinating the preparation of threat assessments to support ACAT I to IV systems.

d. Threat assessments will be written at the lowest possible classification consistent with user needs, but no higher than SECRET. More highly classified supplements will be developed if necessary for program decisions. If a threat assessment must be released to the North Atlantic Treaty Organization (NATO), a specific country, or group of countries, it will be prepared in coordination with HQDA/DIA. The HQDA, TISO will coordinate this effort.

e. The appropriate MACOM headquarters will be responsible for coordinating the preparation of threat assessments to support ATDs, ACTDs and other technology efforts.

f. Approval authorities for threat assessments are indicated in Table 1-1. Threat assessments for ACAT I and II systems will be forwarded through command channels to ODCSINT for review and approval.

g. Draft documents (such as, a MNS, ORD, TEMP, and so on) will be forwarded to the supporting intelligence office for review and approval of the threat statement.

h. ODCSINT will forward threat assessments written for materiel systems requiring DAB review to DIA for validation. In the case of threat assessments prepared for Army-lead SAPs, ODCSINT will coordinate assessments with other Services involved before submitting them to DIA.

i. Threat assessments submitted for HQDA approval will be footnoted, by paragraph, to indicate data sources. Footnoting is required to expedite the review and approval process.

3-10. System threat assessment report (STAR)

a. *General.* The STAR summarizes the approved threat provided to combat and materiel developers for all ACAT 1D or 1C systems (DOD 5000.2-R) and information systems. It provides an assessment of the capabilities of potential adversaries, as to their ability to neutralize or degrade a specific U.S. system, or system concept. It is the primary threat reference to be used in preparation of threat portions of an ORD, IPS, AOA, TEMP, and TTSP. (See table 1-1 for STAR preparation responsibilities and approval authorities.) In the event that an ACAT 1D or ACAT 1C systems (DODD 5000.2-R), automated information systems, or OSD T&E oversight programs is not affected by a threat, then the combat developer may submit a request to waive the STAR. A request to waive the STAR for an ACAT 1C systems (DOD 5000.2-R) or DAB oversight programs will be submitted to the Under Secretary of Defense for Acquisition via the Army Acquisition Executive (AAE). Requests for waivers of STARs for Class I-III automated information systems will be submitted to the HQDA ODCSINT, ATTN: DAMI-FIT. All requests for waiver will be processed through intelligence channels.

b. Timing.

(1) ACAT 1D programs (subject to DAB review at milestones I through IV) and ACAT 1C programs through milestone I (subject to DAB review at milestone I).

(a) *STAR.* The initial STAR is developed by the proponent combat Threat Manager. After MDR I, all subsequent updates will be prepared by the materiel developer Foreign Intelligence Officer (FIO). In all instances, the developer preparing the STAR is responsible for coordinating initial STARs, updates, or changes prior to forwarding to ODCSINT in accordance with criteria established in paragraph 3-10c below.

(b) *Submissions.* The combat developer will prepare and submit an electronic copy (disk or e-mail when practical) of the initial STAR to ODCSINT no later than 180 days following MDR 0. ODCSINT will forward the HQDA approved STAR to DIA for validation within 60 days of receipt, but no later than 60 days prior to the documentation review meeting.

(c) *Updates.* As a minimum, STARs will be updated by responsible developers every 24 months. Additionally, STARs will be updated and forwarded to ODCSINT no later than 120 days prior to the documentation review meeting (now called a Pre-ASARC) for the next MDR. Updates will be in the form of a new STAR or an appendix and will include all intelligence information to be considered by the developer prior to the next milestone.

(d) *Out-of-cycle changes.* When significant changes in the threat occur, especially threat affecting critical system characteristics, and the threat status, STARs will be revised and reissued or changes developed prior to the normal update requirement. Changes will be forwarded for ODCSINT approval and DIA validation per Table 1-1.

(e) *Intelligence report preparation.* Content will be in accordance with guidance in DODI 5000.2.

(2) ACAT 1C programs beyond MDR I (subject to ASARC at MDR II through IV).

(a) *Materiel Developer (MATDEV).* The MATDEV assumes responsibility for STAR preparation beyond MDR I. The materiel developer preparing the STAR is responsible for coordinating STAR updates or changes with the combat developer prior to forwarding to ODCSINT in accordance with criteria established in paragraph 3-10c below.

(b) *Submissions.* Under normal circumstances, the initial STAR will be approved and validated by ODCSINT as of MDR I. Thereafter, updates will be prepared in accordance with criteria in paragraph 3-10b(2)(c) below. ODCSINT will function as the final approval and validation authority for STARs supporting ACAT 1C programs subsequent to MDR I.

(c) *Updates.* As a minimum, STARs will be updated by responsible developers every 24 months. Additionally, STARs will be updated and forwarded to ODCSINT no later than 120 days prior to the documentation review meeting (now called a Pre-ASARC) for the next major decision review (MDR). Updates will be in the form of a new STAR or an appendix and will include all intelligence information to be considered by the developer prior to the next milestone.

(d) *Out-of-cycle changes.* When significant changes in the threat occur, especially threat affecting critical system characteristics, CICs, and the CIC threat status, STARs will be revised and reissued or a change developed prior to normal update requirements. Changes will be forwarded for ODCSINT approval. Subsequent updates will be in accordance with paragraph 3-10b(2)(c) above.

(e) *Intelligence report preparation.* Content will be in accordance with DIAR 55-3 for ACAT 1D.

c. *Structure.* (See app B for an example of a STAR.)

d. *Content.*

(1) *Threat assessments.* Threat assessments will be based on DODIPP threat data sources. Other analyses, however, are acceptable as long as the rationale is included and they are reasonable projections of accepted data. Thus, non-DODIPP data should not necessarily be discarded. Appropriate data can be included in documents that support the acquisition process, as long as it is clearly highlighted and identified as non-DODIPP data. Terms of estimated probability should be used to the maximum extent possible.

(2) *Critical Intelligence Category (CICs).* CICs represent threat capabilities or thresholds established by the program, changes to which critically impact the effectiveness and survivability of proposed systems. CICs normally will be developed by the Program Manager, Product Manager (PM), or materiel developer, with assistance from the supporting Foreign Intelligence Office (FIO), and coordinated with the proponent TRADOC Systems Manager (TSM), or combat developer. The PRs incorporating CICs will be forwarded in accordance with chapter 2 of this regulation. New intelligence bearing on the CICs should be brought to the attention of the PM and the TSM immediately. CICs will be used to focus subsequent STAR changes or updates. Analyst for the Army and Army supported intelligence production centers should have a complete list of all CICs related to each Army Program. When a CIC is breached the Production Center will inform the FIO or Threat Manager telephonically, and publish a topical intelligence article to highlight the significance of their finding, which will include an analysis assessment as to the impact of the breach on the program.

(3) *Appendixes.* Appendixes will be developed as necessary to support assessments made in the body of the STAR.

e. Approval and validation. ODCSINT is the HQDA approving authority for STARs for ACAT I systems (DOD 5000.1) and automated information system (DOD 5000.2-R). CG, AMC; CG, SSDC; CG, USAISC, and CG, TRADOC are respective materiel and combat developer authorities responsible for approving STARs forwarded to HQDA, ODCSINT, DAMI-FIT. A fully coordinated draft STAR with appropriate approval documentation from the combat and/or materiel developer, as appropriate, will be forwarded to HQDA, ODCSINT, DAMI-FIT. The STAR will include a statement signed by the PM or his representative that he has reviewed the document and that the system description is accurate, and the CICs in the STAR reflect the program's critical intelligence needs. (For STARs up to MDR I, the statement will be provided by the proponent materiel developer in coordination with the combat developer.) ODCSINT will obtain DIA validation of STARs for ACAT ID programs-HQDA will validate STARs for ACAT IC programs.

f. Classification. STAR classification will be limited to SECRET. Higher level annexes may be added as needed.

g. References.

(1) A bibliography will be included in the STAR, which will list all data sources used in preparation of the document. Referenced data sources will be the most recent versions.

(2) The STAR will be annotated by paragraph and keyed to the bibliography to show the sources of data. Annotation is required to expedite the approval process; it also will assist in STAR updates and changes.

3-11. STAR ACAT II-IV

All ACAT STARs will be prepared using the STAR format.

a. ACAT II programs (subject to ASARC review at milestones I through IV).

(1) *MDR I.* Through MDR I, the combat developer maintains responsibility for STAR preparation; thereafter, it becomes the responsibility of the materiel developer. In all instances, the developer preparing the STAR is responsible for coordinating the initial STAR, updates, or changes prior to forwarding to HQDA, ODCSINT, DAMI-FIT.

(2) *Submissions.* ODCSINT will function as final approval and validation authority for STARs supporting ACAT II programs. The combat developer will prepare and submit an electronic copy (disk or e-mail) of the initial STA to ODCSINT no later than 150 days following MDR 0.

(3) *Updates.* As a minimum, STARs will be updated by responsible developers every 24 months. Additionally, STARs will be updated and forwarded to ODCSINT no later than 120 days prior to the documentation review meeting (now called a Pre-ASARC) for the next major decision review (MDR). Updates will be in the form of a new STA or an appendix and will include all intelligence information to be considered by the developer prior to the next milestone.

(4) *Out-of-cycle changes.* When significant changes in the threat occur, especially threat affecting critical system characteristics, CICs, and the CIC threat status, STARs will be revised and reissued, or changes will be developed prior to normal update requirements. Changes will be forwarded to HQDA for ODCSINT approval and validation no later than 60 days prior to the next scheduled ASARC.

(5) *STAR waivers for ACAT II programs.* In the event a waiver for an ACAT II program (DOD 5000.2-R) is requested, it will be submitted to the MDA. All requests for waiver will be processed through intelligence channels.

(6) *Intelligence report preparation.* Content will be in accordance with DIAR 55-3. DIA is responsible for ACAT ID report preparation.

b. Content.

(1) *Threat assessments.* Threat assessments will be based on DODIPP threat data sources. Other analyses, however, are acceptable as long as the rationale is included and they are reasonable projections of accepted data. Thus, non-DODIPP data should not necessarily be discarded. Appropriate data can be included in documents that support the acquisition process, as long as it is clearly highlighted and identified as non-DODIPP data. Terms of estimative probability should be used to the maximum extent possible.

(2) *Critical Intelligence Category (CICs)*. CICs represent threat capabilities or thresholds established by the program, changes to which critically impact the effectiveness and survivability of proposed systems. CICs normally will be developed by the Program Manager, Product Manager (PM), or materiel developer, with assistance from the supporting Foreign Intelligence Office (FIO), and coordinated with the proponent TRADOC Systems Manager (TSM), or combat developer. The PRs incorporating CICs will be forwarded in accordance with chapter 2 of this regulation. New intelligence bearing on the CIC should be brought to the attention of the PM and the TSM immediately. CICs will be used to focus subsequent STAR changes or updates. Analyst for the Army and Army supported intelligence production centers should have a complete list of all CICs related to each Army Program. When a CIC is breached the Production Center will inform the FIO telephonically, and publish a topical intelligence article to highlight the significance of their finding, which will include an analysis assessment as to the impact of the breach on the program.

(3) *Appendixes*. Appendixes will be developed as necessary to support assessments made in the body of the STAR.

(4) *Approval and validation*. ODCSINT is the HQDA validation authority for STARs developed for ACAT II programs. CG, AMC; CG, SSDC; and CG, TRADOC are respective materiel and combat developer authorities responsible for approving STARs forwarded to HQDA, ATTN: DAMI-FIT. A fully coordinated draft STAR with appropriate approval documentation from the combat or materiel developer, as appropriate, will be forwarded to HQDA, ODCSINT, ATTN: DAMI-FIT. The STAR will include a statement signed by the PM or his representative that he has reviewed the document and that the CICs reflect the program's critical intelligence needs. (For STARs up to MDR I, the statement will be provided by the proponent materiel developer in coordination with the combat developer.)

(5) *Classification*. STAR classification will be limited to SECRET. Higher level annexes may be added as needed.

(6) *References*. A bibliography will be included in the STAR, which will list all data sources used in preparation of the document. Referenced data sources will be the most recent versions. Also, every STAR will be annotated by paragraph and keyed to the bibliography to show the sources of data. Annotation is required to expedite the approval process; it also will assist in STA updates and changes.

c. ACAT III and IV programs.

(1) *Preparation/Approval/Validation*. The appropriate MACOM headquarters threat support activity will be responsible for coordinating the preparation of threat assessments to support ACAT III and IV programs. Approval and validation for STARs for ACAT III and IV programs through MDR I (Combat Development) is HQ, TRADOC, DCSINT, and after MDR I is HQ, AMC, DCSINT. The threat support activity will forward an information copy of all STARs prepared for ACAT III and IV programs to HQDA, ODCSINT, ATTN: DAMI-ST.

(2) *System threat assessment waivers*. In the event that an ACAT III or IV system or automated information systems will not be affected by the threat, the developer may submit a request to waive the preparation of a STAR for the program. This waiver request will be forwarded through the supporting intelligence organization for coordination and approval. For ACAT III and IV programs, the approving authority for a threat waiver request through MDR I (Combat Development) is HQ, TRADOC DCSINT. The approving authority for automated information systems programs is the HQ, USASC DCSINT. The approving authority for ACAT III and IV programs for a threat waiver request after MDR I, (Material Development) is HQ, AMC, DCSINT. If the waiver is approved, an information copy of the waiver will be provided to HQDA, ODCSINT, ATTN: DAMI-FIT.

3-12. Threat test support package (TTSP)

a. General. The TTSP is based on the STAR but focuses on the particular purpose of the test (such as, a developmental or operational test). A TTSP must provide sufficient detailed intelligence information to enable the tester to accurately portray the threat projected to exist at a post-IOC date. Determination of the threat year and scenario selection will be made by the TIWG on recommendation of the system proponent and evaluation organization.

b. Timing. The TTSP development timeliness will follow documentation timeliness developed during the system's initial TIWG meeting. A TCG will be held within 90 days following the initial TIWG, and TTSP development should begin within 60 days of the TCG. The final approved TTSP must be provided to the tester/evaluator. Continuous coordination between the threat proponent, evaluator, and tester is required.

c. Structure. TTSP format guidance is at appendix C.

d. Preparation.

(1) TTSPs will be prepared for developmental and operational testing of ACAT I-IV systems when an operationally realistic threat is required. Specific testing requirements will be determined by the appropriate TIWG. Determination of the requirement for an operationally realistic threat portrayal will be made by the TIWG on the recommendation of the evaluation organization based on the TEMP requirements.

(2) TRADOC and AMC will coordinate production of the TTSP then TRADOC will prepare all subsequent iterations that support operational test.

(3) AMC will prepare subsequent iterations that support developmental testing.

(4) A TTSP is not required for a developmental or an operational test that does not require replication of threat.

(5) Conflicts related to planned threat portrayals that deviate from the approved threat that cannot be resolved at MACOM level will be referred to HQDA, ODCSINT for resolution.

e. Approval. (Fig 3-5)

(1) ODCSINT approves all TTSPs developed for ACAT I, II and OSD T&E oversight systems. ODCSINT will forward a copy to DIA for review and comment for ACAT 1D and ACAT 1C (through MDR I). (See App C for an example of the TTSP and its validation process).

(2) TRADOC approves all TTSPs developed for operational testing of ACAT III and IV systems that are not on the OSD T&E oversight list.

(3) AMC approves all TTSPs developed for developmental testing of ACAT III and IV systems that are not on the OSD T&E oversight list.

f. Classification. TTSP classification will be limited to SECRET or below. Higher level supplements may be added as needed.

3-13. Analysis of Alternatives (AOA)

a. General. The AOA is a critical document in the acquisition cycle that relies upon the use of modeling and simulation. The threat analysis portion of the AOA references the STAR and determines those elements against which a given system might be used and threat forces that could be used against that system. Determination of the threat year and scenario selection will be made by DCSOPS and ASA(ALT). Scenarios used in the AOA should be based on situations that conform to scenarios in the Defense Planning Guidance (DPG). Underlying assumptions concerning the threat should not conflict with DPG assumptions. (See Table 1-1 for preparation responsibilities of the threat-related sections of the AOA.)

b. Timing. Threat-related sections of the AOA will be prepared and updated as required to meet the milestone decision review process.

c. Structure. The threat-related section's structure and format are dependent on the scope of the AOA. Formats will be determined at the initial TCG.

d. Content. Threat assessment will be based on the STAR and other DODIPP threat data sources. The threat should be provided in sufficient detail to identify, with a reasonable degree of assurance, the conditions that might exist when employing the new U.S. system. As a minimum, the threat-related section should include broad considerations (such as, nature and size of opposing forces or low- versus high-intensity conflicts), as well as detailed inputs (strength of kinetic energy projectile attacks, precision munitions employed, information warfare, precision munition countermeasures employed, and so forth).

e. Approval and validation. ODCSINT is the DA approving authority for the threat-related sections of AOAs for ACAT 1D, 1C and II Programs. ODCSINT will obtain validated ACAT 1C-II AOAs and DIA validation of the threat-related sections of AOAs for ACAT 1D programs. (Fig 3-6)

f. Classification. Threat-related sections of the AOA will be limited to SECRET or below. Higher-level supplements may be added as needed.

3-14. Special Access Programs (SAPs)

a. ACAT I-IV SAP programs require STARs. An information copy of each STAR will be provided to the DAMI-FIT functional branch TISO. Threat support, in addition to that required by this regulation, for Special Access Programs (SAPs) and sensitive activities will be under provisions of AR 380-381. ODCSINT is responsible for recommending to the SAP Oversight Committee (SAPOC) whether a program or activity warrants protection as a SAP. This recommendation will be based on the program security status, the state of similar foreign technology (to include, possible countermeasures), and the threat posed by foreign intelligence services. Program security will be reviewed by INSCOM. Multi-discipline intelligence (MDI) threat data will be furnished to HQDA, ODCSINT (DAMI-CH and DAMI-FIT) and the Working SAPOC by the NGIC and the Army Counterintelligence Center (ACIC). Generally, SAP threat support will be managed in a manner similar to normal acquisition programs. The ability to get the necessary threat producer "access" to the program will determine what deviations are required from the standard procedure. DAMI-FIT will validate the foreign technology assessment as furnished by the appropriate program threat support activity (PM, FIO, TM, or other) as determined by the mission area TISO. The TISO will coordinate all threat support and ensure that a copy of the validated threat assessment is furnished to DAMI-CH prior to the working SAPOC. The TISO will attend program reviews, working meetings and the working SAPOC. If not able to attend, a replacement will be appointed and coordinated with Director DAMI-FI. The TISO, in coordination with the SAP program manager and appropriate threat support activity, will direct the review and distribution of a SAP STAR, STA or intelligence report. Maximum use of technical support from NGIC and approved threat documentation such as STARs for existing programs will be made. ACAT I SAPs programs require a STAR.

b. ACAT II, III and IV SAPs require a STAR. An information copy of each STAR will be provided to and retained by the TISO.

(1) Exceptions to this policy will be requested in writing to HQDA, ODCSINT, ATTN: DAMI-FIT.

(2) Only DIA or HQDA DCSINT validated and approved foreign threat will be presented at the working or final SAPOC. DAMI-FIT will mediate any differences between the PM and NGIC.

Section II

Army Studies

3-15. Army studies

a. Army studies conducted in accordance with AR 5-5 will include a process to identify requirements for threat and intelligence support. This process will apply to each of the eight categories of studies:

- (1) Manpower and Personnel.
- (2) Concepts and Plans.
- (3) Operations and Force Structure.
- (4) Installations and Logistics.
- (5) Science, technology, systems, and equipment.
- (6) Management.
- (7) Intelligence.
- (8) International Security.

b. Study directives and plans prepared by HQDA elements in accordance with AR 5-5, whose goal is to provide policy guidance or implementation will be coordinated in draft with HQDA, ODCSINT ATTN: DAMI-FIT, to ensure that threat ramifications have been considered during the development process.

c. Each study directive or plan will include, as a minimum, a section outlining the potential threats to the process or system that the directive or plan will cause to be developed. The threat section should include a description of the threat that could reasonably be expected, and the conditions or situations where the threats would likely manifest themselves.

d. The SAG sponsor (The Army Staff element, Field Operating Agency, or MACOM responsible for the study) may form a SAG. The SAG will consist of representatives from Army elements having a clear functional interest in the study topic or use of the study results. All SAG's with identified threat and intelligence requirements will have an intelligence representative. HQDA, ODCSINT (DAMI-ST) will provide a representative to SAG's formed for DA directed studies.

e. The SAG chairperson, or study director shall submit PR's per chapter 2 of this regulation for production support through the intelligence staff of the sponsoring agency. If the sponsoring agency has no intelligence staff, the PR will be submitted to DAMI-FI.

f. The Chairperson of the SAG will identify intelligence requirements and will provide a copy of the minutes of each meeting to DAMI-FI.

3-16. Other Army plans and strategy documents

The Army Enterprise Strategy and the Command and Control Protect Program Management Plan will also include a process to identify requirements for threat and intelligence support. Production requirements will be submitted by the proponent SIO in accordance with chapter 2 of this regulation.

3-17. Technology

a. The Science and Technology (S&T) Program covers a very wide range of areas required for defense applications. The basic research and exploratory development stage provide the foundation on which all else is built for development and exploitation of technological opportunities. In response to military needs, or in development of new military capabilities, technology is matured and applications are examined in the advanced development stage in order to establish the feasibility and military utility before acquisition decisions are made. In addition to the normal acquisition issues such as cost, performance, and risk, threat must be included early on in the development and throughout the life-cycle of ACTD, ATD, and other technology efforts.

b. Advanced concept and technology demonstrations (ACTDs) are fieldable brassboard system demonstrations established to provide the basis for evaluation of both acquisition and military utility issues before commitment to major investment and the formal acquisition process. ACTDs are an integral part of the requirements definition process and are driven primarily by user requirements rather than by technologies. During the planning of ACTDs, all factors that are essential to a major acquisition program will be considered, that is, ACTDs represent "vertical" integration. If the user is not prepared to acquire the system ACTDs may be terminated and placed "on the shelf" for later use. If the user does want to acquire the system, the ACTD demonstrator may be fixed to be made suitable for operational use and acquired in limited numbers or, if required in greater numbers, transitioned to the formal acquisition process at MDR I, II, III, or IV as appropriate.

c. Advanced technology demonstrations (ATD) are undertaken to apply technology to military problems. ATDs assess the maturity of technologies and their potential for transition of new concepts into the formal acquisition process at MDR I for new systems or for MDR IV for product improvements to existing systems. ATD technologies may be applied across several systems, that is, "horizontal" integration.

d. Other technology efforts not formally established as either ACTDs or ATDs may have potential application to military systems and may require threat input as appropriate.

e. HQDA ODCSINT, DAMI-FIT, will work closely with the Army Science Board and the Assistant Secretary of the Army for Research, Development and Acquisition to ensure that threat is considered in all ACTDs and as new and emerging technologies are demonstrated in ATD and other technology efforts as appropriate.

f. Army CI will not produce a new threat assessment if two or more previous, recent assessments indicate low FIS or international terrorist threat and no new information indicates a change in the threat assessment level.

3-18. Army Battle Lab

TRADOC established the Army Battle Labs as a means to develop capabilities for a Force Projection Army that begins where battle appears to be changing and that encourages experimentation via simulations and prototypes using real soldiers and real units to determine technology insertion or new requirements. Battle Lab Tenets include conceptual foundation, horizontal technology insertions, science and technology thrusts, Army modernization objectives, across doctrine, training, leader development, organizations, and material (DTLOMS), simulations, involves real soldiers and real units, use of electronic networking, material developer involvement and is linked to Louisiana Maneuvers. HQDA, ODCSINT, DAMI-FIT and the TRADOC, DCSINT must work in coordination with the supporting Threat Office to provide threat support to Battle Labs.

THREAT SUPPORT TO FORCE, COMBAT AND MATERIAL DEVELOPMENT

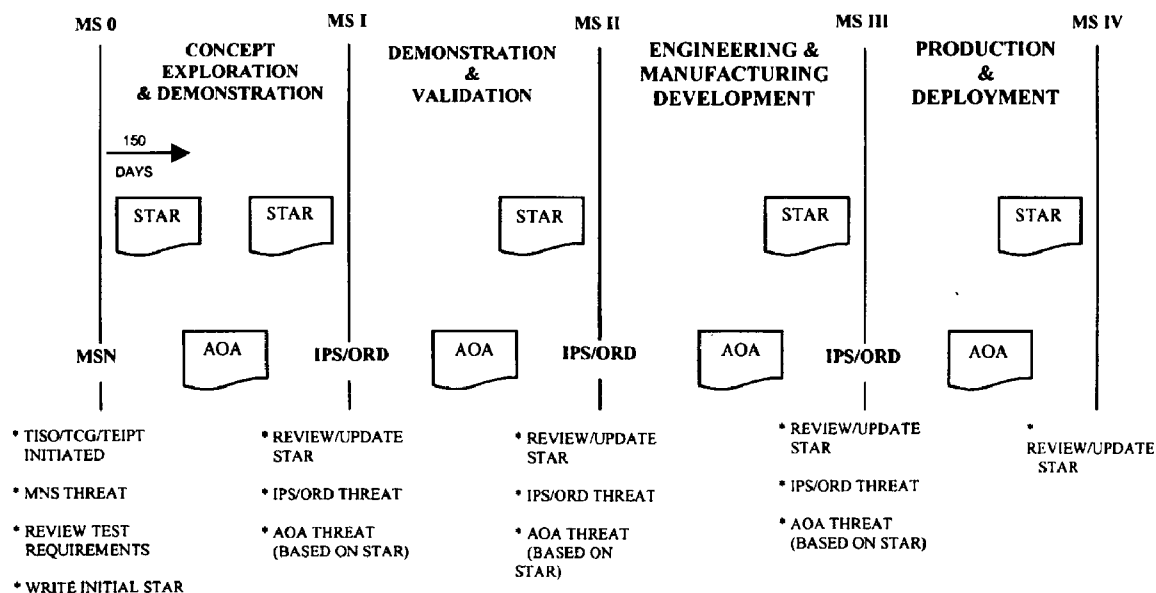


Figure 3-1. Threat support to force, combat, and material development

THREAT SUPPORT TO DEVELOPMENTAL AND OPERATIONAL TESTING

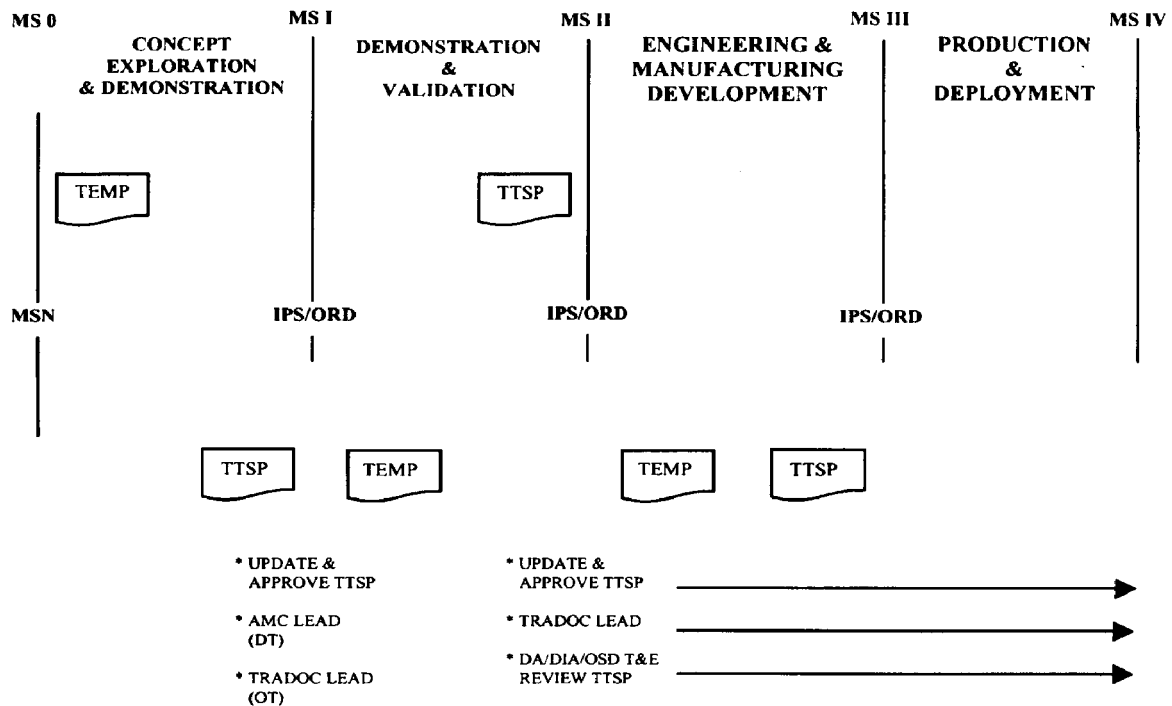


Figure 3-2. Threat support to developmental and operational testing

STAR PRODUCTION & VALIDATION PROCESS (ACAT I PROGRAMS THROUGH MS I)

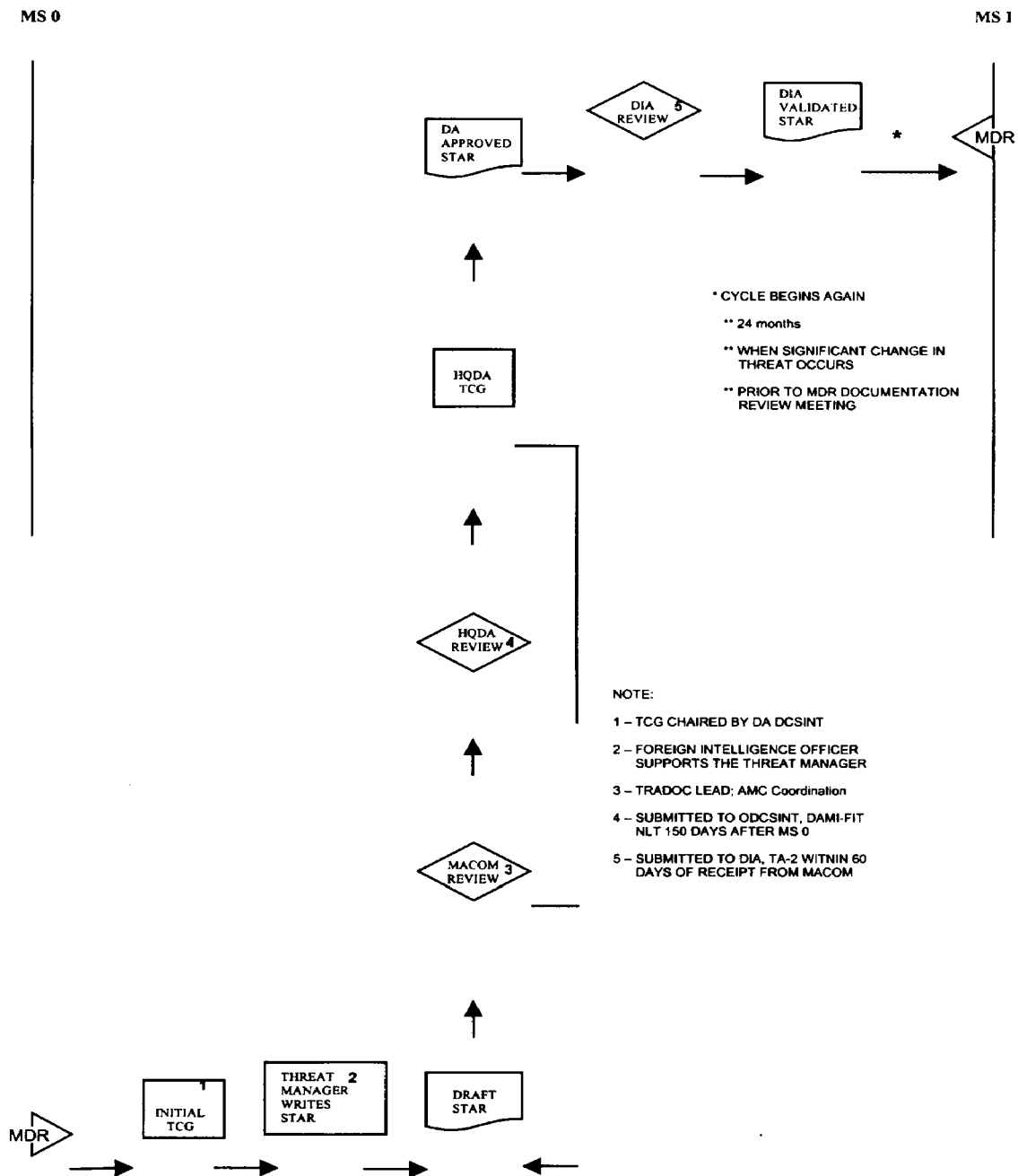


Figure 3-3. STAR production & validation process (ACAT I programs through MS I)

STAR PRODUCTION & VALIDATION PROCESS **(ACAT I PROGRAMS BEYOND MS II)**

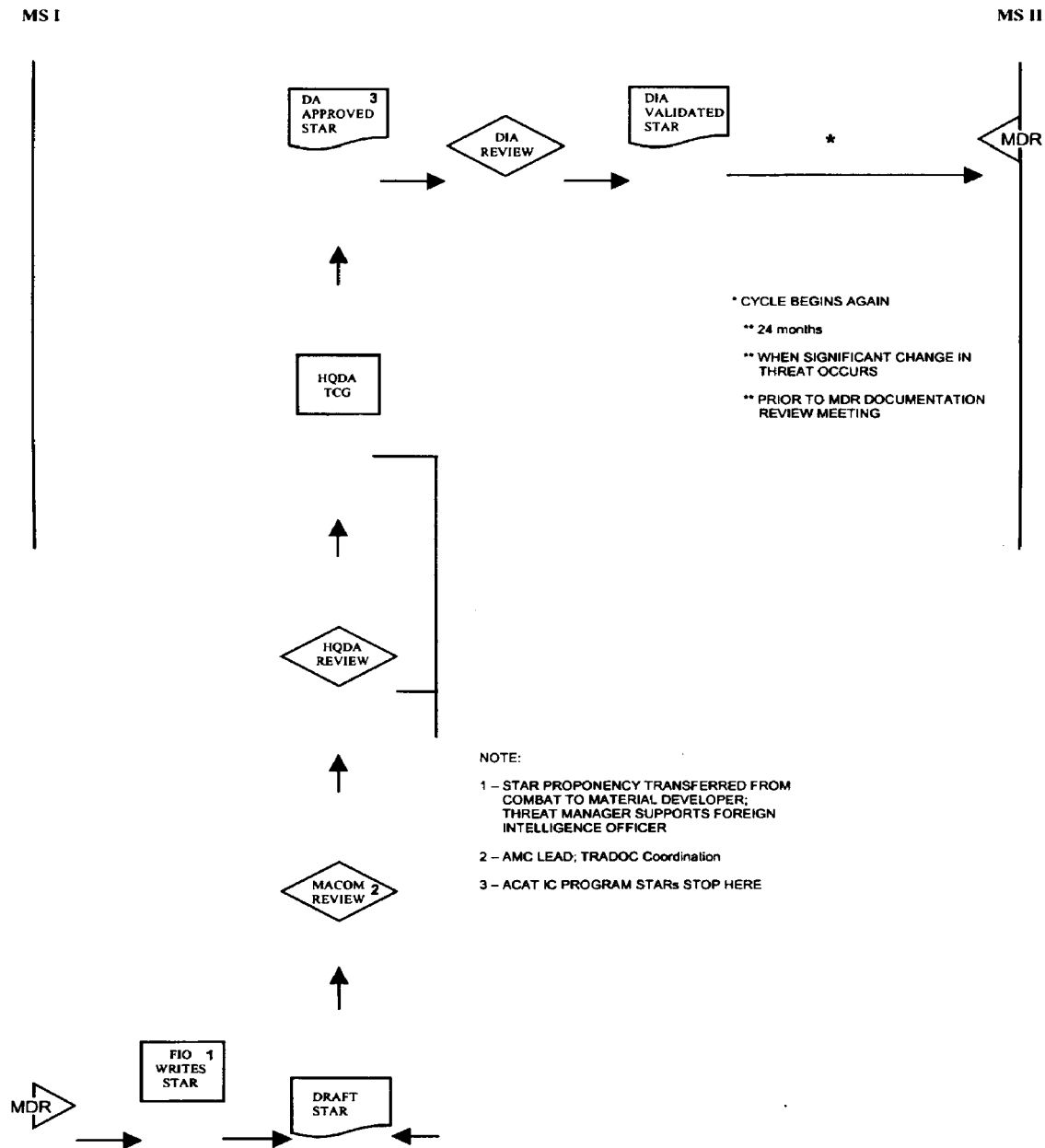


Figure 3-4. STAR production & validation process (ACAT I programs through MS II)

THREAT TEST SUPPORT PACKAGE (TTSP)

VALIDATION PROCESS

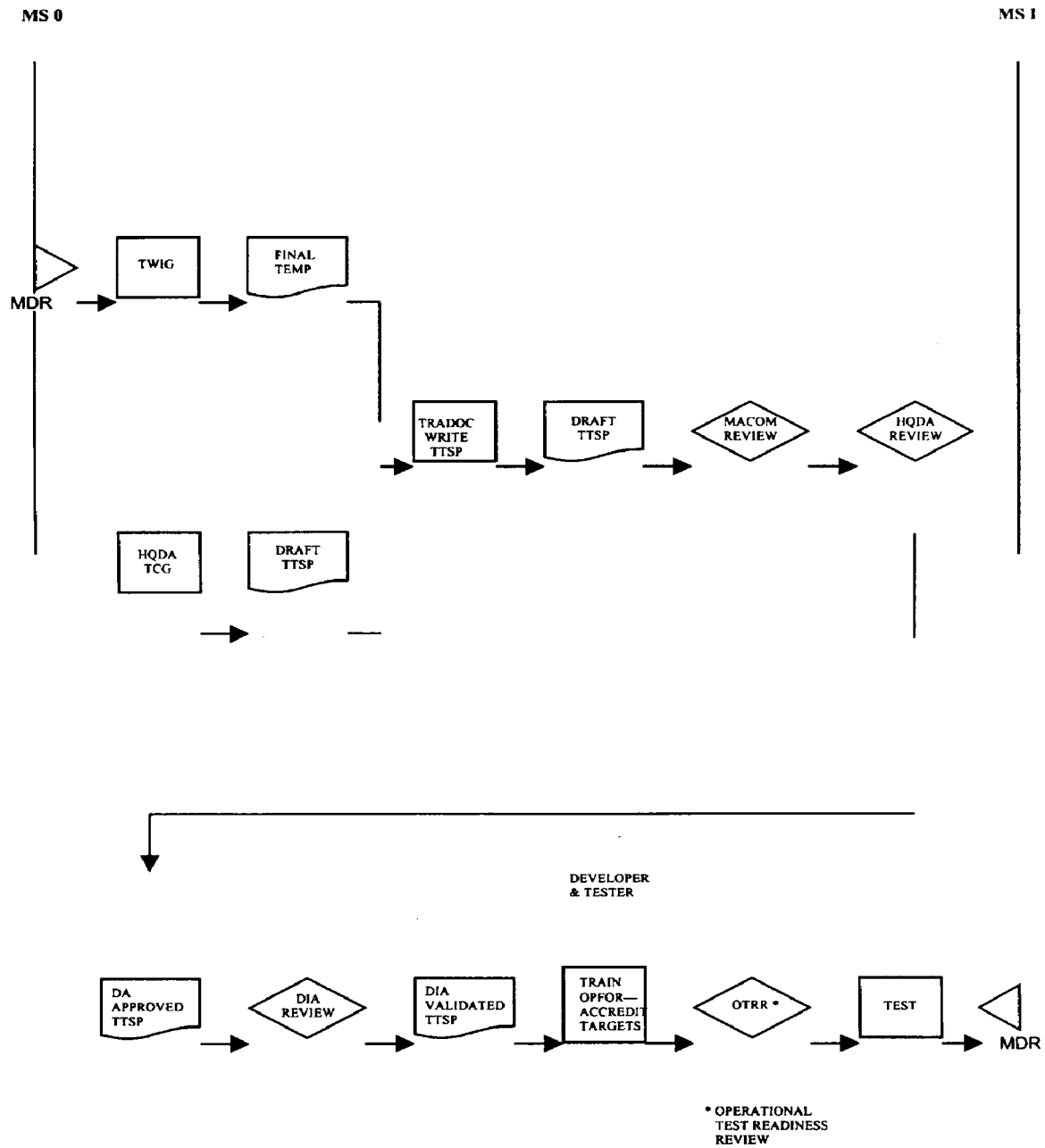


Figure 3-5. Threat test support package (TTSP) validation process

ANALYSIS OF ALTERNATIVES

VALIDATION PROCESS

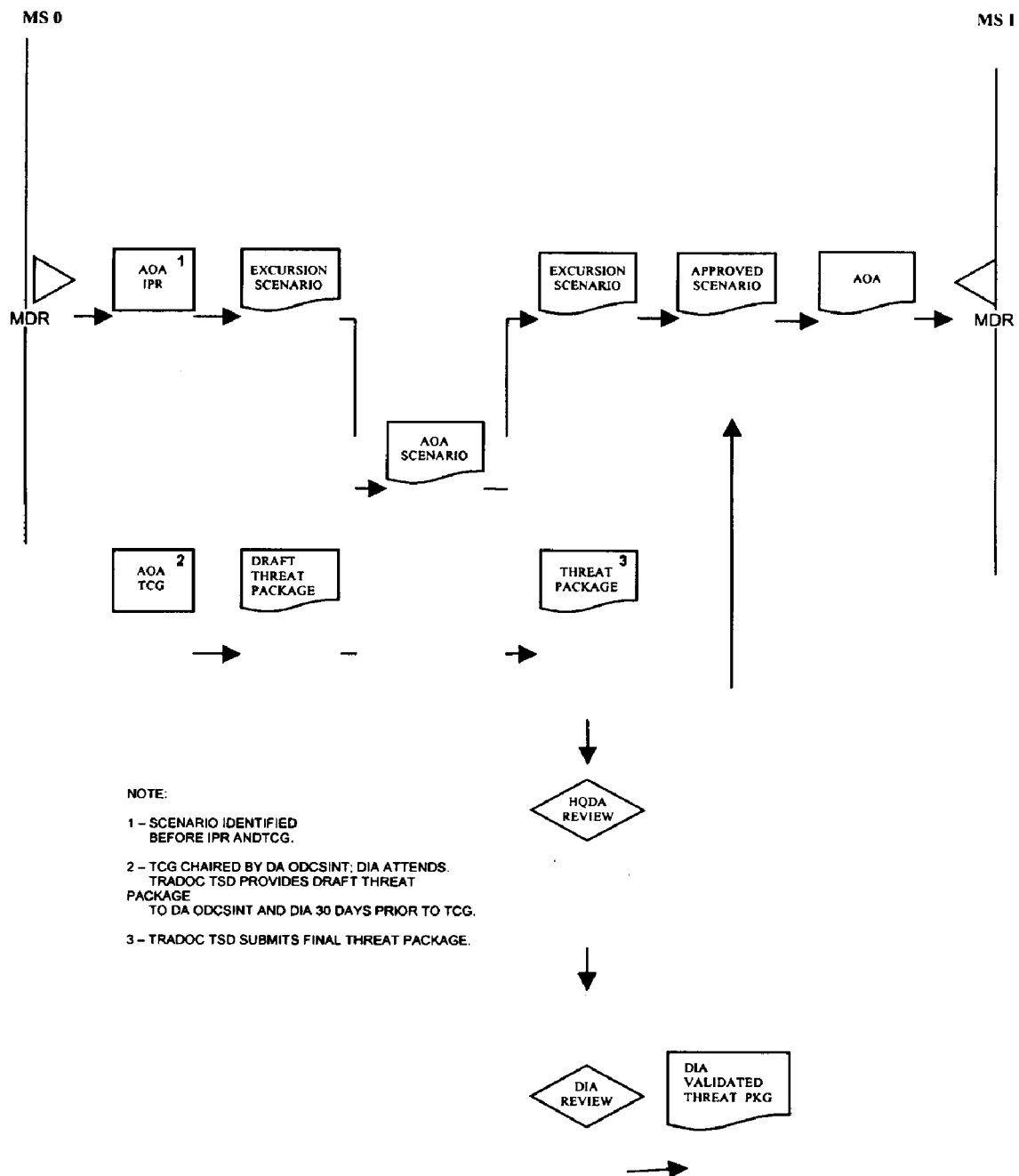


Figure 3-6. Analysis of Alternatives (AOA) validation process

Appendix A

References

Section I

Required Publications

AR 5-5

Army Studies and Analyses. (Cited in para 3-15*a*.)

AR 5-11

Management of Army Models and Simulations. (Cited in para 3-4*a* and 3-4*d*.)

AR 380-381

Special Access Programs (SAPs). (Cited in para 3-14*a*.)

AR 70-1

Army Acquisition Policy. (Cited in para 1-5*b*(3)(c).)

Section II

Related Publications

A related publication is merely a source of additional information. The user does not have to read it to understand this regulation.

AR 1-1

Planning, Programming, Budgeting and Execution System

AR 25-1

The Army Information Resources Management Program

AR 70-1

Army Acquisition Policy

AR 71-9

Material Requirements

AR 73-1

Test and Evaluation Policy

AR 380-5

Department of the Army Information Security Program

AR 381-1

Control of Dissemination of Intelligence Information

AR 381-20

The Army Counterintelligence Program

AR 525-20

Command and Control Countermeasures (C2CM)

DIA Regulation 55-3

Intelligence Support for Defense Acquisition Programs

DA PAM 73-1

Test and Evaluation Procedures Guide

DA PAM 73-5

Operational Test and Evaluation Guidelines

DODD 5000.1

Defense Acquisition

DOD 5000.2–R

Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information Systems (MAIS) Acquisition Programs

DOD 5200.1–R

Information Security Program Regulation

DODI O–5205.7

Special Access Program (SAP) Policy

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

This section contains no entries.

Appendix B

System Threat Assessment Report Format

B–1. General

This appendix provides a standard format for STARs prepared in support of defense acquisition programs. Administrative procedures will specify details for page numbers and references to source documentation. Contents of the STAR itself are discussed in sections covering preliminary (front matter) pages and the STAR body.

B–2. Administrative procedures

a. Cover Page. (See fig B-2.)

b. Page Numbering.

(1) *Cover page.* No number should be used.

(2) *Preface, Table of Contents, Acronyms and Abbreviations, and Executive Summary.* Use lower case Roman numerals (i, ii, and so forth).

(3) *Chapter 1 through 6.* Begin numbering with the chapter-page number (1-1, 1-2, 2-1, 2-2, and so forth).

(4) *Appendixes:* Begin numbering with A-1, A-2, and so on. Use as many appendixes as needed. Examples are listed below.

(a) Appendix A—CIC, CIC threat status, and intelligence production requirements. (Page 1 will be numbered A-1, and so on.)

(b) Appendix B—Tables, drawings, and charts.

(c) Appendix C—Bibliography.

(d) Appendix D—Distribution.

(5) *References.*

(a) *Standard rule:* Every paragraph in chapters 1 through 6 must be referenced by identifying, in brackets, the bibliographical source(s) listed in appendix C. For example, a bracket in [6, 7, 15] implies the source of information for the given paragraph was derived from the 6th, 7th, and 15th entries in appendix C (Bibliography).

(b) *Possible Exception:* Chapter 6 (Likely Reactive Threat), due to the nature of the information therein, may not always have referenced paragraphs. In such instances, the proponent will clearly identify the source of the stated information (for example, analyst comment or conclusion) in brackets following the paragraph—for example [analyst comment].

B–3. STAR preliminary (front matter) pages

a. Preface. A formatted page outlining the scope of the STAR, offices involved in preparation, responsible program office, information cutoff date, and system an milestone identified. When appropriate, DIA and CIA review statements will be included in the STAR. The criterion outlined below applies.

(1) DIA validation statement (ACAT IA, IAM, or other programs subject to DAB review only). Documents for DIA review and validation will include the following statement in final copies of the STAR: “This document is produced by

the (preparing agency), with analytical contributions (list all agencies who provided input to the STAR). The Defense Intelligence Agency has reviewed this document, concurs with its assessments, and validates it for use in (system name) decisions and developments.”

(2) CIA review statement (ACAT IA, IAM, or other programs subject to DAB review only). DIA will forward a copy of each draft STAR to CIA for review and comment, and appropriate CIA comments will be incorporated into the STAR. DIA’s validation package sent back to DA, ODCSINT will contain the CIA comments as an enclosure. Approval must be obtained from both CIA and DIA to incorporate any CIA comments in the STAR. The following statement will be placed in the preface of final copies of the STAR: “The Central Intelligence Agency has reviewed the (system name) STAR and provided (or did not provide) comments for use by DIA or the Army.”

b. Table of contents and list of figures and illustrations.

c. Executive summary. A concise description of the projected future operational threat environment, the system-specific threat, the reactive threat that could affect program decisions, and, when appropriate, results of interactive analysis obtained by the program manager when evaluating the program against the threat. Time frame of the threat to be addressed will start at initial operational capability (IOC) of the program and extend to at least IOC + 10. The executive summary will provide a complete, autonomous threat overview. It will be specific and sharply focused and provide key intelligence judgments applicable to critical intelligence categories and particular milestone issues. (Note: It will specifically identify significant threat changes that have been noted since the last STAR was validated. These threat changes may be related to events such as a breached CIC threshold or otherwise be significant enough to note.) Key intelligence judgments will be identified in a separate subparagraph within the executive summary.

B-4. STAR body

The body of the STAR will focus on relevant major threat capabilities that could impact on the effectiveness of the new U.S. system. The body will consist of the following chapters:

a. Chapter 1 (Introduction). Brief opening statement, to include a short summary of the MNS for the system.

b. Chapter 2 (US System Description). The program TSM or PM will provide the system description for Chapter 2. Summary of program objectives for the system as defined in the ORD, to include mission, available physical and technical characteristics (including such electronic parameters as frequency bands, radiated power, modulation, and so forth), system operational concepts or method of operation, initial operational capability, and life span data (detailed parameters may only become available as the program matures). If development of the system would cause a marked change in the threat to related elements, such as launch platform, associated command, control, and communications (C3), then these elements should be addressed in the system description. (Note: If that marked change is already identified in another document such as a capstone STAR, then a statement that cross-references the other document will suffice.) The minimum acceptable operational performance requirements expected operational environments, critical system characteristics, and system operational and support concepts contained in the ORD should be summarized. The system description section of the STAR must describe the U.S. system in sufficient detail to ascertain what threats may have capability against the proposed system. The following statement should be placed in the system description section of the STAR: “The elements of (enter program name) program protection including sensitive technologies and unique system features, protection threats and vulnerabilities, and program security concept and proposed countermeasures are contained in the program protection plan (PPP). In developing the PPP, the Program Manager has used the information contained in the STAR where appropriate.”

c. Chapter 3 (Operational Threat Environment (OTE)). A generalized overview of the operational, physical, and technological environment in which the system will have to function through at least IOC and IOC + 10 and, if applicable, the targets it is designated to engage. Region, country, or both can break out the OTE. Ongoing political and military changes affecting the threat should be included. Developments and trends that can be expected to affect mission capability during the system’s lifetime should be projected out to the end of the life cycle when possible. Areas covered should include enemy doctrine, strategy, and tactics affecting system missions and operations. Threat content and emphasis will vary from program to program. (Note: The OTE will portray a comprehensive picture of the total aggregate of conditions and influences in which the system will be intended to function. It should include (but not limited to) countermeasures, initial nuclear weapons effects (electromagnetic pulse, radiation, thermal, and blast), nuclear, biological, chemical (NBC) contamination threats.)

d. Chapter 4 (Targets). If applicable, an analysis of actual capabilities and signatures of projected enemy targets (such as vehicles, ships, aircraft, or silos) the U.S. system is designed to engage. The target chapter can be broken out by region, country, or both. Target employment, characteristics, command and control, numbers, and signatures should be included. Types and density of targets might also be covered along with such common parameters as thickness and types of armor to be defeated. Threat characteristics for individual targets, if required, should be placed in appendixes to the basic documents. (Note: The target section will include the full range of targets to be engaged within the mission areas the system is designed to perform. Some STARs might not require a target section. An example would be a satellite-based communications system STAR.)

e. Chapter 5 (System-Specific Threat). An assessment of the threat to the mission capabilities of the system throughout its operational lifetime. The system-specific threat section may be broken out by region and country or by technology. Ongoing political and military changes affecting the threat should be included. Time frames for threat

snapshots are at IOC of the system and at IOC + 10. Threat assessment should integrate doctrine, force level and structure, combat readiness, and means (conventional; electronic; initial nuclear weapons effects; NBC warfare capabilities; advanced weapons such as directed energy weapons used as either threats or countermeasures; or others, as appropriate). Information Warfare (IO) must be included in this chapter. Detail and certainty will decrease as projections extend into the far term. Confidence in key judgments should be expressed in estimated terms to the maximum extent possible. Analysis will be responsive to CICs developed by the PM. CICs are a series of threat capabilities or thresholds established by the program, changes to which could critically impact the effectiveness and survivability of the proposed system.

(1) System-specific threats will focus on threat capabilities that are directly relevant to the mission and performance of the U.S. system. Descriptions of threat capabilities or projections of threat capabilities will be based on approved DOD intelligence or national intelligence when available. Other analyses are acceptable for the far term, so long as the rationale is included and they are reasonable projections of acceptable data.

(2) Conclusions and judgments will be expressed in terms of estimated probability to the maximum extent possible. The assignment of qualifying adjectives to express probability for example the probability of an event occurring, or the existence of capability and intent is an important component of the threat assessment. To achieve consistency in the use of qualifying estimated terminology, the following qualifiers, listed below in decreasing order of likelihood, will be used.

- (a) Near certain (also: will, shall, is expected, or is anticipated): 90 to 99 percent.
- (b) Probable (also: likely, we believe, we estimate, or it is probable that): 65 to 89 percent.
- (c) Possible (also even chance, may, or could): 36 to 64 percent.
- (d) Improbable (also: unlikely or probably not): 10 to 35 percent.
- (e) Slight chance (also: highly doubtful or near impossible): 0 to 9 percent.

(3) The system-specific threat (IOC) checklist includes the following information:

- (a) System description (of opposing weapons).
- (b) Magnitude of threat (projected force level).
- (c) Threat integration combined evaluation of threat to the U.S. system when hostile employment doctrine, force levels, and systems are considered.

(4) Follow-on information on the system-specific checklist includes a snapshot threat at IOC + 10. This section also should assess developments that would serve to degrade the system's capability out to the end of its cycle. Appropriate items are:

- (a) System description.
- (b) Magnitude of threat.
- (c) Threat integration.

f. *Chapter 6 (Reactive Threat)*. To the maximum extent possible, changes that might reasonably be expected to occur in enemy doctrine, strategy, tactics, force levels, technology, and weapons systems (to include advanced weapons such as directed energy weapons) as a result of development and deployment of the new system or disclosure of system technical information.

(1) Analysis of each reactive threat should consider, as a minimum, projections of—

- (a) Modifications in strategy, doctrine, and tactics.
- (b) New systems or modifications to existing systems description and likely deployment.
- (c) Changes in force level.
- (d) Threat integration (combined evaluation of components of potential relative threat to the system).

(2) The reactive threat section will contain both the most likely reactive threat and the technologically feasible threat, broken out by region and country, or both as follows:

(a) The most likely reactive threat provides a best estimate of an adversary's developments based on historical trends, evidence of research and development, perceived military and political-economic requirements, and technological capabilities. The likely reactive threat delineates the system an adversary will most probably develop and deploy during a specified period. Threat options should be defined and any potential for those options to be exercised, presented.

(b) Technologically feasible threat section projects alternatives should the adversary's requirements differ from those assessed most likely from intelligence sources. The technologically feasible threat, although not constrained by intelligence projections, must be consistent with an adversary's technology, economic, and production capabilities. The technologically feasible threat section provides decision-makers with a basis for judgment about the impact on a specific U.S. system if the threat were to evolve in a direction other than that considered most likely by the intelligence community. Potential for projected technologically feasible threats must be discussed.

B-5. Appendixes

Appendixes contain detailed information, generally in tabular form, required by the Service to conduct an interactive analysis or to support statements made in the body of the STAR. Minimum essential appendixes are outlined below.

a. *Appendix A. CICs, CIC Threat Status, and associated intelligence production requirement control numbers will be combined in appendix A.*

(1) *CICs.*

(a) CICs are those threat parameters, generally quantifiable (such as, potential adversary's quantity, type, force mix, and characteristics of actual projected threat systems and technological changes—identified by the combat developer or material developer), that would critically impact on the effectiveness, survivability, security, and cost of an acquisition program. CICs represent “show stoppers” (that is, if breached, would defeat or significantly degrade the ability of the U.S. system to perform its mission). The combat and material developer, in coordination with the supporting TM or FIO, must conduct a detailed analysis of the types of enemy technologies or doctrinal changes that—if they presently exist or are later developed—could degrade the successful development of the program. For example, directed energy weapons (either threats or countermeasures to U.S. systems) could radically impact on personnel and equipment on future battlefields. Military doctrine, tactics, strategy, and expected employment of systems should be considered for inclusion in CICs. CICs also should contain specific parametric values, such as radar cross-section, armor type and thickness, and acoustic characteristics that highlight U.S. system vulnerabilities in relation to an adversary's capability.

(b) There should be a direct correlation between CICs and the system's critical system characteristics. CICs must be developed in sufficient detail to provide the intelligence community a clear idea of exactly what information is needed. They are not general statements of interest; rather, they should address specific thresholds. Normally, a CIC will have a numeric value; rarely should it be answerable with a “yes” or “no” response.

(c) CICs must be developed for the initial STAR. Updates to the STAR will focus on intelligence relevant to them. Examples are provided in figure B-1.

(d) If no CICs are identified, a statement to that effect will be included in the CIC appendix.

(2) *CIC Threat Status (CTS).* For each CIC, an assessment of its threat status (CTS) will be provided. The CTS will be a stand-alone synopsis and will include the status of foreign threat programs, technology, and research efforts, along with a projection of capabilities and potential for breach of the CIC threshold. In addition, intelligence data required for in-depth analyses—such is found in scenarios for gaming, lengthy technical descriptions, vulnerability studies, or table of organization and equipment (TOE)—should be consistent with the main body of the STAR and placed in appendixes or separately published documents. If these separately published documents are intended to supplement the STAR, they must be validated by DIA.

(3) *Intelligence production requirements.*

(a) Once the CICs are developed, each will be converted to a separate PR. If two or more CICs are closely related, they may be included in one PR.

(b) The TM/FIO will register their PR using COLISEUM. Either the validated PR control number or the preliminary MACOM control number will be indicated for each CIC listed in the STAR.

(c) All intelligence echelons, including DIA and DA ODCSINT, must ensure that new intelligence bearing on CICs is brought to the attention of the PM in a timely manner.

(d) The TM/FIO will process PRs as prescribed in Chapter 2 of this regulation.

b. *Appendix B. Tables, Drawing, and Charts.*

c. *Appendix C.* A bibliography reference list of current and major sources used in the preparation of the report. These sources should mainly include DIA-validated intelligence data sources. Other sources should be clearly identified as not validated data sources. Preface those sources not DIA-validated with an asterisk (*), and include a footnote specifying that asterisks imply that sources are not DIA-validated.

d. *Appendix D.* Distribution to appropriate DOD component and DA level offices should be included.

-
1. (Classification) Evidence of multispectral obscurants being fielded that are capable of degrading or defeating the (type) infrared sensor in the (number) micron (far) infrared band.
 2. (Classification) Evidence of fielding (type) jammers, decoys, or mufflers that could degrade or defeat the (type) sensor in the (no.) Hz bandwidth.
 3. (Classification) Evidence of fielding IR camouflage, signature suppression devices, decoys, or jammers that could degrade or defeat the (number) sensor in the (no.) to (no.) micron bands.
 4. (Classification) Evidence of fielding a high-power microwave (HPM) weapon operating in the (no.) to (no.) GHz range.
 5. (Classification) Evidence of armor protection levels that exceed (no.) mm or rolled homogeneous armor for top surfaces.

Figure B-1. Critical Intelligence Category (CIC) examples

(SYSTEM NAME)

SYSTEM THREAT ASSESSMENT REPORT (STAR)

APPENDIX __ / ANNEX __

} [if applicable]

TO



(CAPSTONE SYSTEM)

PREPARING AGENCY:

INFORMATION CUTOFF DATE:

APPROVED/VALIDATED BY: (DA) / (DIA)

[As appropriate]

DATE APPROVED/VALIDATED: (DA) / (DIA)

[As appropriate]

PUBLICATION DATE (DRAFT OR FINAL):

(CLASSIFICATION)

NATIONAL SECURITY INFORMATION

Unauthorized Disclosure Subject to Criminal Sanctions

CLASSIFIED BY:

DECLASSIFY ON:

Figure B-2. STAR Cover page (format)

Appendix C Threat Test Support Package (TTSP) Format Guidance

C-1. General

a. When a threat is to be used during testing such as an ATD, ACTD, concept development, simulation, developmental, or operational test, a TTSP must be prepared. If a validated threat portrayal is required for the test, appropriate command and or agencies must review, approve and validate the TTSP. If a validated threat is required for the test, the threat portrayal during the test must also be validated.

b. The TTSP is the threat baseline document for the testing community for a specific test. The purpose of the TTSP

is to identify the threat requirements for the specific test, describe the threat to be portrayed, and describe how the threat fits into the overall test execution and evaluation requirements.

c. The base document for the threat to be reflected in the TTSP is the STAR. Also, the threat environment for the TTSP should be as realistic as possible, and should be drawn from the threat scenario to be portrayed during the test. If the STAR is inadequate to provide detailed threat portrayal to satisfy threat test specific requirements; additional threat documentation can be utilized for inclusion in the TTSP after review and approval through the TCG process.

d. The TTSP is prepared by the designated proponent threat office for the test. Input is received from the TEIPT, tester, evaluation, proponent, and program TAWG. A generic outline of the process to follow in preparing the TTSP should include:

(1) TIWG initial meeting—Establishes threat year and the region of the world and possibly the scenario to be used as the backdrop for testing.

(2) TCG initial meeting—after the initial TEIPT is conducted; a TCG should be convened as soon as possible. The TCG chair should be the point-of-contact from the highest approving threat intelligence command or agency. Normally, TCG participants include a representative from: DIA, HQDA, ODCSINT, ATEC Threat Coordination Office, the Program Executive Officer/Program/Product Manager, TRADOC DCSINT, TRADOC TM proponent, AMC, DCSINT FIO proponent, AMSAA, Intelligence Production Centers (NGIC/NAIC/MSIC), OTSA, PM ITTS, ARL, Big Crow, and/or joint proponents. If the system to be tested is a major automated information system, or interfaces with a fixed information system that falls under the proponentcy of HQ, USASC, then the USASC, DCSINT should also participate in the TCG. This meeting should be used to establish the basic threats, targets, and simulator to be portrayed during testing.

(3) TAWG initial meeting—after the initial TCG, a threat accreditation-working group (TAWG) should be convened. The TAWG chair should be identified during the initial TCG. Normally, for DT, the chair would be TECOM, for OT the chair will be from ATEC, for technology efforts such as ATDs, ACTDs, for advanced warfighting experiments, and Red Team efforts, the chair would be HQDA, ODCSINT.

C-2. Format

The following format should be followed when preparing the TTSP. All sections will be completed for each TTSP. This format is appropriate for all developmental and operational tests, whether conducted as Force-on-Force (FOF) field portrayals, in constructive simulation, or virtual simulations.

a. TTSP preliminary pages.

(1) *Title page.* This page shows the title, preparing agency, information cutoff date, U.S. system project office, the MACOM or DA validation date, as appropriate.

(2) Tables of contents and illustrations.

b. Threat test documentation.

(1) Type of test and ACAT.

(a) TEMP approval date.

(b) OTP approval date.

(c) TEP approval date. (Test Evaluation Plan and/or Test Operations Plan)

(2) *Evaluation agency.* Provide full mailing address with POC's name and telephone number.

(3) *Test organization.* Provide full mailing address with TTSP POC's name and telephone number.

(4) *TRADOC proponent school.*

(a) Provide full mailing address of threat organization with POC's name and telephone number.

(b) Provide full mailing address of the TRADOC Systems Manager (TSM) with POC's name and telephone number.

(5) *Test location.*

(a) Location of the test site. Provide the site location with the full mailing address and the POC's name and telephone number.

(b) World location being represented.

(c) TRADOC approved scenario used as a basis for test vignettes.

1. This section of the TTSP needs to be cross-walked with the operational requirements document (ORD) and the Alternatives of Analysis (AOA) requirements.

2. The TTSP should include limitations identified in the TRADOC approved DPG scenario and in simulations to clarify potential differences in outcome data from the test.

(6) *Initial operational capability (IOC) of system to be tested.* Crosscheck with the DPG approved scenario for the blue system. If a difference in dates results in a significant difference in the threat portrayal, a brief notation of those differences should be identified in this section. If a difference in dates results in a significant difference in Blue portrayal, a brief notation of those differences will be made in this section.

(7) *Threat year.* Cross-check with the DPG approved scenario for the threat systems. If the threat date of the test is different from the year being played in the DPG approved scenario, you need to identify and distinguish both dates. If

a difference in dates results in unexpected portrayal outcomes, a brief notation of those differences and outcomes should be identified in this section.

(8) *Title and date of threat assessment.* Include the title and date of the threat assessment, (STAR) in this section. Also, identify the command/agency who prepared and validated the threat assessment.

(9) *TTSP approval dates and sequence.* This page identifies a sequence of the agencies and/or command(s) that conducted a review of the TTSP (and sections within the TTSP) and the date those commands and/or agencies approved the TTSP.

(a) *Test plan document date.* The TTSP prepares needs to review and coordinate with the tester for threat resource requirements in the test plan. The items to be reviewed include both personnel and equipment to be portrayed in the test.

(b) *AMSAA date.* Reviews final draft of the TTSP with respect to weapons/munitions, countermeasures (red and blue effects), and certifies their data. AMSAA POC, mailing address, and telephone number should be identified here.

(c) *TAWG report date.* Depending on the type of test, ATEC, AMSAA, TECOM, or HQDA, final approval of TAWG report for all threat simulators and/or surrogates to be utilized in the test. The following items should also be included:

1. Include TAWG chair person's name, mailing address and telephone number.

2. Include dates, locations, and subjects when TAWG committee meets.

(d) *PM date.* Reviews and concurs with the draft TTSP to insure adequacy to support test execution and evaluation requirements. The PM concurrence can be accomplished at a TEIPT or an early Test Readiness Review (TRR).

(e) *TSM date.* Reviews and concurs with draft TTSP to insure adequacy to support test execution and evaluation requirements. The TSM concurrence can be made at a TEIPT or an early TRR.

(f) *Tester date.* Reviews and concurs with draft TTSP to insure adequacy to support test execution requirements. The tester concurrence can be made at a TIWG or an early TRR.

(g) *Evaluator date.* Reviews and concurs with draft TTSP to insure adequacy to support test evaluation requirements. The evaluator concurrence can be accomplished at a TIWG or an early TRR.

(h) *TRADOC proponent School/Center date.* Completed TTSP for review, approval, and validation. Include dates, locations, and subjects when TCGs were held.

(i) *TRADOC DCSINT date.* Reviews and validates for ACAT III and ACAT IV acquisition programs. For ACAT I and ACAT II acquisition programs, reviews, approves for TRADOC, and sends to HQDA, ODCSINT for review, approval and validation.

(j) *HQDA, ODCSINT date.* Reviews and validates for ACAT IC and ACAT II systems. For ACAT 1D, reviews, provides HQDA approval and coordinates DIA approval/validation.

(k) *DIA Date.* Reviews and validates final TTSP for ACAT 1D and all other acquisition programs with OSD oversight.

(10) *Threat portrayal approval dates for operational testing (OT).*

(a) *Approval of threat training.* TRADOC DCSINT is the approval authority for threat training for OT. This approval certifies that the "threat" has been trained to portray the threat correctly during OT. A memorandum approving threat training is provided to the combat developer with an information copy to the PM, the test community, and to the threat community. The memorandum approving threat training is not normally provided until the threat proponent and/or other commands/agencies who are involved with threat portrayal during OT, each certify their own training and test readiness. This memorandum is normally provided during the OTRR 3 meeting.

1. *Proponent school approval.* The TRADOC proponent school/center threat POC for the OT certifies overall threat training has been provided, execution during training is representative of the threat to be portrayed during OT, and that the threat forces are ready to proceed to OT. This certification is provided in a memorandum to TRADOC DCSINT.

2. *Other commands/agencies approval.* An example, of this would be if OTSA was involved in the test, a letter certifying their equipment and/or personnel met the threat test requirements, required of OTSA to execute/portray for OT. This certification is provided in a memorandum to TRADOC, DCSINT. An example of organizations that could be included in this section are; joint proponents, OTSA, ARL, Big Crow, and PM ITTS.

(b) *Approval of threat readiness to begin an OT.* This is a memorandum from TRADOC, DCSINT to the combat developer, with an information copy to the PM, Test Community and the Threat Community stating that the threat is ready to proceed to OT. This statement may include a review of limitations and/or issues for the threat, which impacts or restricts threat portrayal during the OT.

(c) *Approval of threat portrayal during OT.* This is a memorandum from TRADOC DCSINT to PM, TSM, ATEC-OEC, containing the final validation of the threat actually portrayed in OT. Threat portrayal was/was not performed to the expectations identified in the TTSP and threat portrayal during test trails was adequate to support test evaluation. A mention of the trials that were/were not approved during the testing is appropriate. The memorandum needs to include a statement that the proponent threat office and TRADOC DCSINT need to review and comment on the final test report.

c. *TTSP body.*

(1) *Section I. Test system identification.*

(a) *Description of system.* The TSM and/or the PM supplies a description of the system to be tested to the preparer of the TTSP. It should include the technical parameters and the tactical application of the system to be utilized in the test. If the TSM or the PM does not provide technical and tactical information, then the threat preparer's will not be able to adequately develop the TTSP in enough detail to satisfy test requirements. The TTSP should not begin until full system description and tactical information about the system to be tested is provided to the threat preparer.

(b) *Organization or concept of the system.*

(c) *Doctrinal employment and tactics of the system.*

(d) *Description of system/subsystem situations to be portrayed in the OT.*

(2) *Section II. Test issues and criteria.* Test issues and criteria are the primary basis for determination of whether a validated operational threat environment (OTE) is required for the test. These issues are furnished to the tester for inclusion in the Operational Test Plan (OTP). The threat integrator (TTSP author) must coordinate these issues with the tester and evaluator to determine the extent of the OTE required to answer the issues.

(a) *Test COICs from System Evaluation Plan (SEP).* COICs are prepared by the Combat Developer and furnished to the tester and evaluator. The criteria and rationale will provide the primary indication that a validated TTSP will be required. Generally, if lethality and vulnerability or survivability are at issue, an OTE supported by a validated TTSP would be required. Detailed coordination with the tester and evaluation is necessary to determine the extent of the threat portrayal required to answer the issues.

(b) *Explanation of threat requirements for each appropriate COIC.* Based upon the review mentioned in the aforementioned paragraph, provide a generic, but complete explanation of the expected threat to be portrayed and how the threat will be portrayed during the test.

(3) *Section III. Threat.* This section provides background information on what threats will be portrayed during the test. There is no need to include threats that will not be portrayed. If for example, only threat tanks are required for the test; identify only the threat tank platforms to be included into the threat vignettes and the tanks weapons and munitions to be portrayed. Do not include in this example, air defense systems and EW equipment if they are not to be portrayed.

(a) *Threat systems.* This section describes what threat systems/subsystems will be portrayed versus blue systems/subsystems during the OT. This includes weapons systems as well as non-weapon systems such as trucks. Items such as EW equipment target acquisition means, and transportation need to be addressed in this section if they are to be portrayed in the test.

(b) *System/subsystem platforms.* When completed, this section should be cross-checked with the following appendixes: D, F, G, H, and J. This section needs to be coordinated with AMSAA early in the test-planning phase.

(c) *Description.* Describe the system and/or subsystem that are appropriate to the threat portrayal requirements for the test. This is a technical review of system/subsystem capabilities required to be portrayed during the test, other than the information described in the two paragraphs below. Intelligence estimates of system/subsystem vulnerabilities would be identified here.

(d) *Weapons.* Describe the weapon system that will be portrayed in the test. Cross-check this section to Appendix D, Fire-Target Matrix and other appendixes as appropriate.

(e) *Munitions.* Describe the munitions to be used, from the weapon systems listed above that will be portrayed in the test. This should include such data as basic loads, rates of re-supply and rates of fire and target acquisition means (day and night). Cross-check this section to Appendix D, Fire-Target Matrix and other appendixes as appropriate.

(f) *Units.* Identify and describe what units will be portrayed (per scenario) under the conditions to be portrayed during testing. Be sure to identify other units that must be accounted for in order for the "test" unit to function. An example would be a transportation unit so that resupply to the artillery unit could be sustained with ammunition during the attack.

(g) *Organizations.* Identify how the threat units are organized in the force structure of the threat country's scenario. There is a need to identify both horizontal and vertical units as is appropriate to the test.

d. *Threat doctrine, operations, tactics, and techniques, procedures and or profiles.* This section describes how the threat units being relocated in the test will conduct its military operations. This information is appropriate for the test because we should replicate as close as possible how we believe the enemy will fight during the test. If for example, this test is about Special Forces (SF), then Threat SF doctrine, operations, and tactics should be described to support the threat portrayed during the test.

e. *Threat countermeasures (CM).* Identify the CM to the system/technology effort to be tested.

(1) Technical CM.

(2) Tactical CM.

f. *Threat targets.* This section is for tests that require no threat to the blue system, only targets for the blue system to attack or to disrupt. This section lists the following:

(1) Test.

(2) Platforms.

(3) Unit/Organizations.

g. *Bibliography.* When using information from a source in the bibliography, use at the end of the paragraph source number and page (for example, 4-36) represents source 4 in bibliography, page 36 within the source document.

h. *Section IV. Appendixes:*

(1) *Appendix A. Test Concept.* This document is provided by the tester. The test concept is developed by the evaluator and tester from the SEP, which is prepared by the evaluator. It will describe, in detail, test scope and criteria. Test concept will be used to define the required threat for a specific test. Approved issues are found in the SEP.

(2) *Appendix B. Scenario.* The scenario is the same as described in the preliminary page. The description of the scenario is a more detailed situation (Background) that sets the stages for why the test vignettes are constructed (why the threat needs to be portrayed as such) to support test evaluation. Scenario. Test scenario describes how the test operations should be conducted. Selection of the scenario is the responsibility of the test proponent. The test organization, in coordination with the TRADOC threat support office, is responsible for integrating the approved threat into the scenario. Normally, test scenarios are based on TRADOC approved low- or high-resolution scenarios or other recent and related combat developer actions. All aspects of the scenario must be reviewed from the threat perspective to ensure adequate portrayal in support of the stated test issues and criteria. Areas to consider include scheme of maneuver, TOE organization and types of equipment, tactics and supporting fires or forces.

(3) *Appendix C. Description of trails, test, runs, or vignettes.* This appendix describes how the threat operations will be conducted. The TTSP must include a description of threat forces and operations that will be used to portray the scenario during the test. Templates showing threat force locations, routes of movement, and listings of threat force organizations and equipment to be used in the test are required. Inclusion of this information allows reviewing agencies to determine whether or not the threat will be portrayed accurately to support the COIC or exit criteria and AOIC. Also, mention the pilot test in this paragraph.

(4) *Appendix D. Fire-Target Matrix.* Completion of Appendices A thru C and an analysis of the munitions in section III, allows the TTSP author and the tester to develop a fire-target matrix. The matrix is restricted to those firers and targets that will be replicated during the test. It will be coordinated with the evaluator and system proponent prior to final submission. The completed matrix will provide the basis to request Ph and Pk data. This request is usually made to AMSAA by the tester. The developed data replicating the lethality of the threat systems should be returned to DAMI-FIT for review by a TCG for validation prior to tester use.

(5) *Appendix E. Threat Targets, Threat Simulators, Model/Simulation, TAWG, UVA, and Surrogates.* Most field-testing requires the use of U.S. Army, NATO, or contractor equipment to be used, in lieu of actual threat systems. Assessments are to be limited to features that are applicable to the specific test. For example, if test threat systems are to be immobile during a test, then it is not appropriate to point out that surrogate systems are not as fast as the actual threat system is attempting to portray. Accreditation reports pertinent to the targets and simulators will provide assessments and limitations for specific use.

(6) *Appendix F. Limitations.* Test proponent and test agency are required to make known overall limitations of the test, such as tactics, equipment, or considerations that should have been in the test but are excluded for whatever reason. The preparer is required to assess and describe the effects of these stated limitations, plus any limitations they perceive, on the ability of the test to portray a valid threat.

(a) *Test limitations.* The tester and the evaluator provide this. Identification of these limitations are required as they pertain to threats ability to portray or conduct a validate threat.

(b) *Threat, test limitations.* These limitations are specific threat issues that cannot be portrayed, but should be portrayed during test. After each item listed, describe the potential impacts the limitation has on the threat and the test as appropriate.

(c) *TAWG, equipment limitations.* This is provided by the TAWG report. The TAWG report will define the threat equipment limitations to be used in the test and any tactical deviation required to offset the equipment limitations.

(d) *Threat data limitations.*

(7) *Appendix G. Threat Force Training Plan.* A threat force training plan is mandatory for force-on-force tests or tests involving any threat replication requiring threat player personnel. The proponent will develop a threat force training plan to train designated player units in threat tactics and situations to be portrayed in the test. The threat force training plan will include a program of instruction (POI). Lesson plans are not required for inclusion into the TTSP, but may be necessary to use in training the actual unit. The POI should be based on what the test threat force needs to know for the specific test.

(8) *Appendix H. Minimum start trial criteria (MSTC) & the rules of engagement (ROE) as required. (See AR 73-5.)*

(9) *Appendix I. Threat data as required. (See AR 73-5.)*

(10) *Appendix J. Record of threat portrayal conducted in trials, test, runs or vignette as required. (See AR 73-5.)*

(11) *Appendix K. OT Live-fire T&E phase.* If the Live-fire T&E is to be included in the test documentation process all Live-fire T&E information is included in this appendix. This should be discussed in the TCG and TAWG meetings as separate tests. It is possible for this appendix to be approved/validated separately from the TTSP.

(12) *Appendix L. TAWG report.* There is no need to include the TAWG report with this document; however, a short discussion of the TAWG final report should be included. The following information should be included; Agency responsible for the report, POC name, address, and telephone number, date of final report, and the date when the TAWG report was presented to the TIWG chairperson.

Glossary

Section I Abbreviations

AAE

Army Acquisition Executive

ACAT

Acquisition category

AFMIC

Armed Forces Medical Intelligence Center

AMC

US Army Materiel Command

AMSAA

Army Materiel Systems Analysis Activity

AMSMP

Army Model and Simulation Management Program

AOA

Analysis of Alternatives

AOIC

Additional Operational Issues and Criteria

APIN

Army Priority Intelligence Needs

APINCG

Army Priority Intelligence Needs Coordinating Group

ARSTAF

Army Staff

ASARC

Army Systems Acquisition Review Council

ASA (RDA)

Assistant Secretary of the Army (Research, Development, and Acquisition)

C2W

Command and Control Warfare

CAA

Concepts Analysis Agency

CAC

Combined Arms Command

CBTDEV

Combat developer

CIA

Central Intelligence Agency

CIC

Critical intelligence category

COIC

Critical Operational Issues and Criteria

COTS

Commercial-off-the-shelf

CRRS

Customer requirements registration system

CTC

Combat Training Center

CTS

CIC threat status

DA

Department of the Army

DAB

Defense Acquisition Board

DAE

Defense Acquisition Executive

DFM

Dissemination Functional Manager

DIA

Defense Intelligence Agency

DIAR

DIA Regulation

DOD

Department of Defense

DODIIP

Department of Defense Intelligence Production Program

DODI

DOD Instruction

DODIC

Department of Defense Intelligence Community

DODIPC

Department of Defense Intelligence Production Community

DPG

Defense Planning Guidance

DPM

Dissemination Program Manager

DT

Developmental Test

FAMTSCEN

Family of Threat Scenarios

FDTE

Force development testing and experimentation

FIO

Foreign Intelligence Officer

GOSC

General Officer Steering Committee

HPM

High-power microwave

HTI

Horizontal Technology Integration

IITF

Information Infrastructure Task Force

INSCOM

US Army Intelligence and Security Command

IOC

Initial operational capability

IPR

Intelligence production requirement

IPS

Integrated Program Summary or Illustrative Planning Scenario

IR

Infrared

IW

Information Warfare

JP

Joint Program

JSAP

Joint Service Acquisition Program

LRRDAP

Long-range research, development and acquisition plan

MACOM

Major Army commands

MAISRC

Major Army Information System Review Council

MATDEV

Materiel developer

MDCI

Multi-discipline counterintelligence

MDAP

Major defense acquisition program

MDR

Milestone decision review

MNS

Mission need statement

MSC

Major Subordinate Command

MSIC

Missile and Space Intelligence Center

NATO

North Atlantic Treaty Organization

NBC

Nuclear, biological, chemical

NDI

Non-developmental item

NGIC

National Ground Intelligence Center

NMISC

National Military Intelligence System Center

ODCSINT

Office of the Deputy Chief of Staff for Intelligence

ODCSOPS

Office of the Deputy Chief of Staff for Operations and Plans

OPFOR

Opposing forces

OPSEC

Operations Security

ATEC

Operational Test and Evaluation Command

ORD

Operational requirements document

OSD

Office of the Secretary of Defense

OSD T&E

Office of the Secretary of Defense Test and Evaluation

OT

Operational Test

OTE

Operational threat environment

OTSA

ATEC Threat Support Activity

PEO

Program Executive Officer

PM

Program, project, or product manager

POI

Program of instruction

POM

Program Objective Memorandum

PPP

Program Protection Plan

PR

Production Request

RDA

Research, development, and acquisition

RDTE

Research, development, test and evaluation

RFP

Request for proposal

S&TO

Scientific and Technical Intelligence Officer

SAG

Study advisory group

SAP

Special Access Program

SAPOC

Special Access Program Oversight Committee

SCI

Special compartmented information

SIGINT

Signal Intelligence

SI

Statement of Intelligence Interest

SIO

Senior intelligence officer

SSO

Special Security Office

SST

System specific threat

SECDEF

Secretary of Defense

SMDC

US Army Space and Missile Defense Command

SSG

Special study group

S&TI

Scientific and technical intelligence

STA

System threat assessment

STAB

Scientific and Technical Assessment Bulletin

STAR

System threat assessment report

STOW

Synthetic Theater of War

STOW-E

Synthetic Theater of War-Europe

STRAT MID

Military Intelligence Detachment (Strategic)

STRICOM

US Army Simulations, Training, and Instrumentation Command

STF

Special task force

TAP

The Army Plan

TASC

Threat Assessment Scenario Committee

TAWG

Threat accreditation-working group

TCG

Threat coordinating group

T&E

Test and evaluation

TEMA

Test and Evaluation Management Agency

TEMP

Test and Evaluation Master Plan

TEP

Test evaluation plan

TISO

Threat Integration Staff Officer

TIWG

Test integration working group

TM

Threat Manager

TOE

Table of organization and equipment

TRADOC

US Army Training and Doctrine Command

TSM

TRADOC System Manager

TTSP

Threat test support package

USD(A)

Under Secretary of Defense (Acquisition)

VWG

Validation working group

Section II**Terms****Accreditation**

Process of determining the extent to which the simulator or target supports the requirements of the specific test or evaluation.

Acquisition categories (ACATs)

Categories established to facilitate decentralized decision making and execution and compliance with statutorily imposed requirements. Categories determine level of review, decision authority, and applicable procedures.

Ad hoc production

A response to a new and unique customer intelligence need. Ad Hoc production must be associated with a production requirement.

AIPP

Army Intelligence Priorities Process. A process which established intelligence priorities based on our customers' stated needs. The basis for intelligence focus and resources for Army, and for articulating Army intelligence needs to DoD and the National Intelligence Community.

AIPP

Army Intelligence Priorities Process. A process which established intelligence priorities based on customers' stated needs. The basis for intelligence focus and resources for the Army and for articulating Army intelligence needs to DoD and the National Intelligence Community.

AIPSP WG

Army Intelligence Priorities for Strategic Planning Working Group. An 0-6 level working group whose main responsibility is to recommend intelligence priorities to the DCSINT and to report the commands assessment of intelligence support to his priority intelligence needs (PIN) at quarterly production reviews. Representatives from MACOMs DCSINT, DA ODCSINT, ODCSOPS and other DA Staff elements represent intelligence interests.

APIN

The Army Priority Intelligence Needs. This priority intelligence needs represent general topical areas of intelligence needed to the conduct of the Army title 10 mission and are developed by DA DCSOPS and DA DCSINT, with inputs from all Army MACOMs having title 10 responsibilities.

APINCG

Army Priority Intelligence Needs Coordinating Group. An 0-6 level coordinating group whose main responsibilities are to prioritize MACOM and Army staff priorities for intelligence support. The Commanders' assessment of intelligence support will be prebriefed to the APIN CG prior to the brief by the Army DCSINT to the Chief of Staff Army (CSA).

APINL

The approved list of APIN by the CSA.

Approve

Within the context of this regulation, the term "approve" signifies the formal or official acceptance or sanction of a threat assessment or product at the intermediate level of authority. For example, an ACAT II program STAR would require approval by the appropriate MACOM and validation by DA ODCSINT. (See validate.)

ARMS

The Army Requirements Management System. A relational database software program used by the Department of the Army to record, and track all intelligence production requirements.

Army Systems Acquisition Review Council (ASARC)

Top-level DA corporate body for systems acquisition that provides advice and assistance to the Secretary of the Army and the Army Acquisition Executive.

Automated Information System (AIS)

An AIS is the automation subset of an information system and represents the use of general-purpose computer equipment. An AIS does not include embedded computer resources designed into material systems by the material developer. An AIS normally consists of a combination of information, hardware (computer), components (monitor, keyboard, modem, printer, display, etc.), software, and telecommunications resources that collect, record, process, store, communicate, retrieve, and display information, such as personnel systems, financial systems, and inventory control systems.

Battle Lab

Battle Labs are a means to develop capabilities for a force projection Army that begins where battle appears to be changing. Tied to our evolving Battlefield Dynamic Concepts and warfighting doctrine in the new FM 100-5, Battle Labs use the battlefield as a reference. By encouraging experimentation via simulations or prototypes, Battle Labs determine requirements in the areas of doctrine, training, leader development, organizational structure, materiel, and soldier support. Since resources realities will curtail most new starts, material requirements will be primarily in the form of technology insertions. By focusing on horizontal integration of technology across the force, Battle Labs will further conserve resources.

Collaborative production center

The production center, which contributes to a production effort by providing a primary producer responses to a Production Requirement, associated with their area of production responsibility.

COLISEUM

Community On-line Intelligence System for End Users and Management.

Combat developer

Command or agency that formulates doctrine, concepts, organization, materiel requirements, and objectives. Represents user community in materiel acquisition process.

Combined Arms Tactical Trainer

An Army non-system training device program for training collective battlefield tasks (primarily at battalion and below) through the use of large scale simulator networking to provide virtual battlefield environments. Consisting of five training simulators: CTT (Close Combat), FSCATT (Fire Support), AVCATT (Aviation), ADATT (Air Defense), and ENCATT (Engineer). CCTT will replace the M1 and M2 simulator currently fielded.

Combat Training Center Program

Provides realistic joint service and combined arms training. It is designed to provide units the most realistic battlefield available-primarily in the "live simulation" environment. Four Components: National Training Center, Combat Maneuver Training Center, Joint Readiness Training Center, and Battle Command Training Program.

Constructive

Mathematical models used as a tool to support collective training (battalion commanders and staffs through Army Theater-Corps Battle Simulation (CBS), Combat Service Support Training Simulation System (CSSTSS), Battalion Brigade Simulation (BBS) and in individual training. May be used with or without human interaction. Sometimes referred to as war game models.

Coordinate

Process of seeking concurrence from one or more organizations or agencies on adequacy of specific draft assessment, estimates, or reports. Intended to increase product's factual accuracy, clarify its judgments, and resolve disagreements on threat issues.

Cost and operational effectiveness analysis (COEA)

Analysis of estimated costs and operational effectiveness of alternative materiel systems to meet mission need and associated program for acquiring each alternative.

Critical Intelligence Categories (CICs)

Threat capability or threshold established by program manager, changes to which could critically impact on effectiveness and survivability of proposed system. CICs serve to alert supporting intelligence organizations regarding specific priority intelligence requirements, in order for them to focus intelligence production and collection efforts.

Critical intelligence categories threat status (CTS)

Status of threat programs, technologies, and research efforts relative to CIC. Will include projection of threat capabilities and potential for breaching CIP thresholds.

Defense Acquisition Board (DAB)

Senior DOD acquisition review board, chaired by USD(A).

Defense Intelligence Production Community

The Defense Intelligence Production Community key players include the Defense Intelligence Agency, service production centers (NGIC, NAIC, NAVMIC), Unified Command Joint Intelligence Centers, Components, Reserve organizations, National Security Agency, and the National Imagery and Mapping Agency.

Distributed

Separate simulations each hosted on a computer and connected via communication networks to create a shared battlefield.

Distributed Interactive Simulation (DIS)

A synthetic environment within which humans may interact through simulation(s) at multiple sites networked using compliant architecture, modeling, protocols, standards and databases.

Dynamic Environment

The environment is constantly changing as a result of man-made efforts (battlefield smoke) and natural phenomenon (weather).

Emulator

A physical model or simulation which duplicates the behavior, properties, or performance of another system. Emulators are frequently used to generate input for other model and simulations.

Force development

Integration of allocated and projected Army resources into time-phased program to develop force properly organized, equipped, trained, and supported to carry out Army missions and functions worldwide. Includes force planning, programming, analysis, structuring, and combat and training developments.

Information System (IS)

Organized assembly of resources and procedures designed to provide information needed to execute or accomplish a specific task or function. It applies to those systems that evolve, are acquired, or are developed that employ information technology. Information system equipment consists of components (for example, hardware, software, firmware, products, or other items) used to create, record, produce, store, retrieve, transmit, disseminate, present, or display data or information.

IFC

Intelligence Functional Codes. A list of intelligence topics broken out in levels each of which addresses a subtopic under the main heading. There are currently 19 basic topics.

Initial operational capability (IOC)

First attainment of the capability to employ effectively a weapon, item of equipment, or system of approved specific characteristics, and which is manned or operated by an adequately trained, equipped, and supported military unit or force.

Instrumentation

The use of electronic or electromagnetic systems to sense and record events performed by real weapons systems, communications systems and personnel. Instrumentation includes detection, measurement, recording, telemetry and data processing.

Integrated program summary (IPS)

DOD Component documents prepared and submitted to MDR authority in support of MDRs I-IV. Succinctly highlights status of a program and its readiness to proceed into the next phase of the acquisition cycle.

Interactive

Two applicable definitions: (1) different simulations and or simulators electronically linked to act together and upon one another; and (2) the iterative processing of information between humans, instrumented equipment and simulations (referred to sometimes as a “warrior-in-the-loop”).

Intelligence

Product resulting from the collection, processing, evaluation, analysis, integration, and interpretation of all information concerning one or more aspects of foreign countries or areas. Intelligence information evaluated in developmental process is referred to as “threat”.

Intelligence community document

Finished intelligence product published under sponsorship of the Director for Central Intelligence and coordinated by various members of the intelligence community, to include DCSINT. Examples are national intelligence estimates and Weapons and Space Systems Intelligence Committee documents. CIA-produced documents are not intelligence community documents.

Intelligence production requirement (IPR)

Stated need for production of intelligence on general or specific subjects, programs system, or weapon.

Intelligence report

A report provided by appropriate intelligence agency or command to milestone decision authority prior to each MDR. For MDR 0, for example, report will confirm validity of the threat contained in the MNS; for MDRs I-IV, report will confirm validation of STA(R) used in support of acquisition program and will address threat issues, risks, or unresolved threat concerns affecting program.

IPSP

Intelligence Priorities for Strategic Planning. Joint Strategic Planning System (JSPS) support document, which identifies countries and intelligence categories and established priorities for DoD intelligence support. Services and CINCs are responsible to input their priorities into this system. The Executive Agent is the J-2. The Army IPSP will feed the DoD IPSP.

IPSP categories

Broad topics of intelligence interest that are expressed in terms intelligence information needs for military planning, programming, budgeting, and decision making.

Joint program

Defense acquisition system, subsystem, component, or technology that involves formal management or funding by more than one DoD Component during any phase of the system’s life cycle.

Live

Real equipment and soldiers operating in the field, such as, an exercise at the National Training Center, but short of an actual conflict.

Major defense acquisition program (MDAP) (ACAT I)

Acquisition program not a SAP and that is—

- a. Designated by USD(A) as a MDAP
- b. Or estimated by USD(A) to require the following:

(1) Eventual total expenditure for RDTE of more than \$200 million FY80/approximately \$300 million FY90 constant dollars.

(2) Or eventual total expenditure for procurement of more than \$1 billion FY80/approximately \$1.8 billion FY90 constant dollars.

Materiel developer

Command or agency responsible for research, development, and production of system in response to approved requirements.

Materiel system

Item, system, or all systems of materiel; includes all required system support elements.

Mission need statement (MNS)

Statement of operational capability required to perform an assigned mission or to correct deficiency in existing capability to perform mission. Identifies USD(A) mission area and describes mission area need. Supports milestone O decisions, and contains threat to be countered. Threat will be derived from DIA-produced or -validated documents.

Model and Simulation

A model is a physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process. A simulation is the operation or exercise of the model overtime. Also, a technique for testing, analysis, or training in which real-world systems are used, or where real-world and conceptual systems are reproduced by a model.

Multi-Discipline Intelligence (MDI)

All source Intelligence, derived from all intelligence disciplines (including those falling under the classic counterintelligence discipline), that could present a threat to a system or systems development process, technology based effort, or NDI/COT procurement.

NGIC

National Ground Intelligence Center.

NMIPC

National Military Intelligence Production Center.

Non-major defense acquisition program (ACAT II-IV)

Program other than MDAP or SAP. (Threat support procedures for ACAT II-IV programs are listed in Table 1-1 of this regulation.)

Object orientated combat simulations

A software design methodology that results in the battlefield being represented by objects which encapsulate associated methods or procedures and where objects communicate by message passing. Examples of battlefield objects are platoons (unit level), tanks (platform level), main guns (component or module level), and gun barrels (part level). Object oriented designs have inherent modularity; for example, to change a tank model only the tank object must be changed.

Operational requirements document (ORD)

Document containing performance (operational effectiveness and suitability) and related operational parameters for proposed concept or system. Submitted to milestone decision authority in support of milestone I through IV reviews. Summarizes threat to be countered and projected threat environment. Threat will be derived from DIA-validated STAR for all ACAT I programs through milestone I and for ACAT 1D programs for milestone II through IV. STAR will be referenced in ORD.

PCR

Production Center response is the primary production center's response provided to the customer's SIO regarding how that center will address the Production requirement.

Primary Production Center

The Production center that has lead production responsibility for a product.

PR

A production requirement. A standardized format in which a requestor states his need for new intelligence production.

Production

Conversion of information or intelligence information into finished intelligence through integration, analysis, evaluation, and interpretation of all available data and preparation of intelligence products in support of known or anticipated user requirements.

Reactive threat

Changes that might reasonably be expected to occur in hostile doctrine, strategy, tactics, force levels, and weapon systems as a result of development and deployment of the U.S. system.

Scheduled Production

A response to a production requirement that includes both recurring and one-time products.

Signatures

A distinctive characteristic of a system. Signatures may be visual, electromagnetic, acoustic, infrared, and so forth. Also, a signature may have an active or passive characteristic that distinguished it from its environment.

SII

Statement of Intelligence Interest. Used to disseminate intelligence information to support customers' areas of interest.

Simulation

To feign or to obtain the essence of a threat, without the reality of warfare. In the distributed interactive simulation (DIS) domains, everything short of actual combat is a simulation. Three categories are live, virtual and constructive.

Simulator

Generic term used to describe family of equipment used to represent threat weapon systems in development testing, operational testing, and training. Threat simulator has one or more characteristics which, when detected by human senses or man-made sensors, provide appearance of actual threat weapon system with prescribed degree of fidelity.

SIO

Supporting Intelligence Office. An office or designated individual responsible for obtaining intelligence required by the command.

Special access program (SAP)

Highly sensitive, classified acquisition program that complies with policies and procedures specified in DOD Instruction 5000.2 for acquisition category of programs with equivalent dollar value. Specific deviations to these policies and procedures must have concurrence of milestone decision authority, which may waive milestone documentation requirements. STARS and other threat-related documents prepared for highly sensitive classified programs are handled administratively in the same manner as other programs, unless special security arrangements are necessary. Special access clearances for these programs will be kept to a minimum.

Standard

A rule, principle, or measurement established by authority, custom, or general consent as a representation or example.

STRAT MID

A small Army Reserve team normally headed by a Colonel war-traced to a strategic intelligence organization performing intelligence functions for that organization.

Synthetic Environments

Internet simulations that represent activities at a high level of realism from simulations of theaters of war to factories and manufacturing processes. They are created by a confederation of computers, connected by local and wide area networks and augmented by realistic special effects and accurate behavior models. They allow visualization of and immersion into the environment being simulated.

System developer (SD)

The term used in the life-cycle management of information systems to represent the Material Developer designation classically used in weapons systems development and threat/tactical system acquisition. The SDs within the Army is AMC, PEOs and USAISC (AR 25-3).

System threat assessment report (STAR)

Threat assessment tailored to and focused on a particular ACAT system. Contains integrated assessment of projected enemy capabilities (doctrine, tactics, hardware, organization, and forces) to limit, neutralize, or destroy system. Will serve as basic threat document supporting system development and will reference DIA-validated threat data sources. A dynamic document that will be continually updated and refined as a program develops. Required for MDRs I-IV. Will be approved and validated in support of ASARC/DAB review.

Target Array

An aggregation of target components that represents one or more essential aspects of the threat for an exercise, test, or simulation. Targets may range from mock-ups that resemble the actual threat visually from a distance or they may emit certain signatures that mimic the threat (for example, infrared, electromagnetic, or acoustic emissions, and so forth). A target array is composed of expendable resources that may be used once and destroyed in the exercise or simulation.

Technologically feasible threat

Potential threat that may be assessed as unlikely but for which capability exists and which would impact on U.S. system under development.

Terrain (Static/Dynamic)

Dynamic terrain allows for terrain changes to be introduced during a simulation. Examples are engineer efforts, building construction or destruction, weather. Static terrain does not change after simulation has been started.

Test and evaluation master plan (TEMP)

Overall planning document used to depict structure and objectives of test program. Provides framework within which to generate detailed test and evaluation plans and to determine schedule and resource implications associated with test and evaluation program.

Threat

a. Ability of an enemy or potential enemy to limit, neutralize, or destroy effectiveness of current or projected mission, organization, or item of equipment. Statement of that threat is prepared in sufficient detail to support Army planning and development of concepts, doctrine, training, and materiel.

b. Statement of a capability prepared in necessary detail, in context of its relationship to specific program or project, to provide support for Army planning and development of operational concepts, doctrine, and materiel.

Threat Accreditation Working Group (TAWG)

Group formed to accredit specific test application of threat simulators, targets, surrogates, and target arrays.

Threat Array

An aggregation of threat components that represents the essential aspects of the threat for an exercise, test, or simulation. For example, an integrated air defense node component of simulated (hardware and software simulations/simulators) radar vehicles, C3 vehicles, surface-to-air missile systems and affiliated support vehicles could be a threat array for a practical exercise, test, or simulation.

Threat assessment

Evaluation of enemy's or potential enemy's current or projected capability to limit, neutralize, or destroy the effectiveness of a mission, organization, or item of equipment. Involves application of threat analysis to specific mission, organization, or item of equipment within context of a military operation. Threat assessments consider product of threat analysis vis-a-vis a US force and include perceived military judgments of evaluated threat force.

Threat coordinating group (TCG)

Group formed to manage threat support to combat and materiel development process throughout entire life cycle of systems process.

Test integration working group (TIWG)

Acquisition program working group chaired by PM and convened at PM's discretion, responsible for establishing and defining test conditions and applicable scenarios (year, region, targets, and arrays) in support of program testing. Representation typically consists of representatives from US System PM, ODCSINT (HQDA), Threat Support Activities, Operational Test And Evaluation Command (ATEC), Combined Arms Center (CAC) Threats Directorate, and Army Materiel Systems Analysis Activity (AMSAA). Principal threat integrator for TIWG is supporting AMC FIO. PM ITTS and NGIC are represented on TIWG when discussions and test planning warrant their participation.

Threat support activity

Provides threat support to a combat, materiel, or systems developer (such as Threat Managers (TMs) in TRADOC; Foreign Intelligence Officers (FIOs) in AMC; and Assistant Chief of Staff for Intelligence (ACSI) for SSDC; and the Deputy Chief of Staff for Intelligence (DCSINT) for USAISC).

Threat test support package (TTSP)

A document of group of documents that provide comprehensive description of threat to US systems being tested and targets the system will engage.

Validate (Threat Documentation)

Within the context of this regulation, the term "validate" signifies formal or official acceptance or sanction of a threat assessment or product at the highest level of authority. Validation certifies the assessment or product as the official version or edition. For example, a STAR for an ACAT 1D program would require approval by HQDA, ODCSINT and validation by DIA. (See approve.)

Validation

The process of certifying that a customer's requirements are consistent with and necessary for the accomplishment of the customers' mission.

Validation (M&S)

The process used to identify, document, and analyze the differences between a given threat simulator and the system it represents.

Validation Office (VO)

It is the single officer; a small office or a self contained intelligence organization that has been established for each Service, each Unified Command and the National Military Intelligence Production Center.

Validation working group (VWG)

Group formed to determine whether threat simulator or target provides sufficiently realistic representation of corresponding threat system and justifies the start or continuation of its development, acceptance, or modification. Chartered by TEMA.

Validation and accreditation plan for threat simulators and targets

Plan that defines and prescribes concepts, processes, policies, and procedures employed in validation and accreditation of threat simulators, targets, and target arrays.

Virtual

Simulators interacting within a virtual reality environment and possible with other simulators. Operational examples are the M1 and M2 found at various Army posts. Future examples will be the Combined Arms Tactical Trainer.

Section III**Special Abbreviations and Terms**

This section contains no entries.

UNCLASSIFIED

PIN 041100-00

USAPA

ELECTRONIC PUBLISHING SYSTEM

OneCol FORMATTER .WIN32 Version 1.12

PIN: 041100-00

DATE: 08-22-00

TIME: 12:45:57

PAGES SET: 65

DATA FILE: C:\WINCOMP\mark.fil

DOCUMENT: AR 381-11

DOC STATUS: NEW PUBLICATION